industrial security

VOL. 2, NO. 4

OCTOBER, 1958

Special Supplement

1958

CONVENTION/SEMINAR

Special Report

"THE SCIENTIST, THE ENGINEER AND SECURITY"

OFFICIAL PUBLICATION OF THE american society for industrial security

PRESIDENT A. T. DEERE

1957 - 1958

CONTENTS

"INDUSTRIAL SECURITY" is published quarterly by the American Society for Industrial Security, Investment Building, Washington 5, D. C. Printed in U. S. A. Application for acceptance as controlled circulation publication is pending at Washington, D. C. Subscription price $2.00 per year, domestic and foreign.

Additional copies of this "Special Report" are available through the ASIS national office for $1.00 each.

"SECURITY AND UNITED STATES TECHNOLOGICAL PROGRESS"
A Panel Discussion and Forum

Remarks of ROBERT L. APPLEGATE, *Office of the Secretary of Defense*

On behalf of the Office of the Secretary of Defense I certainly am pleased to have been invited to participate in this discussion. I think The American Society for Industrial Security is to be complimented on its efforts, its forward thinking, and I might add also, its courage for bringing together several of us today in our combined thoughts on this important subject—a subject which we frankly admit at times has been a little controversial.

In almost any human endeavor, whether striving on the part of one person or toward the common goal of many persons, there is often the strong difference of view regarding the road that should be taken. Naturally, the more important the role is and the wider the range of activity necessary for its accomplishment, the more pronounced may be the road to be selected. Thus we meet today to discuss Security and United States Technological Progress. The goal of course is our nation's defense and defense of the entire free world. The security that we are talking about is the Industrial Security Program of the Department of Defense, that of the Atomic Energy Commission, or any other program which for any reason may place some limitation on those who are engaged in research and development of new weapons and subsistence.

The United States technological progress, as used here, must of necessity refer to that progress which has or can be gained in attaining the many new devices being developed or produced to help assure the adequate defense of our country and that of our world neighbors. Some leading scientists and engineers from time to time have looked upon security as a barrier to the achievement of our fullest possible technological progress. Within the Department of Defense we certainly have not been insensitive to this view. From time to time we have attempted a number of things to reduce the seriousness of this difference of view.

I am sure all of us will agree that history will stand through the years since the turn of the century as the Miracle Years of Technological Progress. We have truly moved into another world during this period. The great bulk of this progress under the American system of free enterprise has moved forward and to a large extent has been inspired by the proper motive, a pure and respectable motive. . . .

Industry today is involved in all kinds of research, both basic and applied and all made possible in one way or another by our preventive system of free enterprise. To serve its end industry has vast research organizations within which has been brought together the most complete modern equipment possible and where the best talents available have been assembled.

The utility of the end items produced through this means and their value in the market place affects the survival in many instances of the sponsoring company. Think of your television programs today: "Progress is our most important product," "Better things for better living through chemistry." This is a reflection of the very things to which I have been referring, and industry long ago realized the advantages of secrecy in handling formulas and new processes. Today, with this tremendous investment committed to exploring new fields, the importance of secrecy has correspondingly increased. . . .

I have a bright nephew who can probably be described as an up-and-coming physicist. He is three years past his doctorate and has had fine experience in those three years. He looks with complete disdain upon the Department of Defense's Security Program, and at times I even suspect a slight degree of contempt in his very enthusiastic attitude or non-enthusiastic attitude. I am not at all familiar, however, with what he does. He is employed, along with many others of his kind, by an enterprising company that feels that their competitive position can best be maintained or kept in hand by keeping secret the efforts of their research staff. This situation certainly is not uncommon.

Further along this line, a week or so ago in the mail I received an interesting brochure just released by one of our major automobile companies. It was entitled "Talk is Expensive." Oddly enough it was addressed to the company's employees urging them not to talk to anyone about the company's new products or any other company business.

Now Mr. Quarles stated that forty per cent of the research efforts in the United States is for defense. Undoubtedly a substantial part of this is surrounded by secrecy. I am sure that a substantial part of the remaining sixty per cent of research also is surrounded by secrecy. In the one instance the purpose is the defense of our country; in the other it is for the purpose of protecting a company's competitive position, its prestige, and of course its anticipated profit.

Despite the desire of some that it be otherwise, secrecy seems to be an essential ingredient of industrial and commercial enterprise, especially in the field of research and development. Compromise of secrets, whether they are company secrets or defense secrets, destroys advantages that flow from research and development. The advantages are too vital to our competitive system, but, more importantly, they are too vital to our national defense to be thrown away.

Remarks of DR. RAYMOND J. SEEGER, *Deputy Assistant Director, National Science Foundation*

What I wish to stress particularly at this time is the significance of the individual scientist, the importance of freedom for his imagination. Science is not quite the prosaic process that some would make out. The scientist is akin to the poet, the maker. Our great scientists have all had a highly imaginative sense.

It is my thesis that blanket security which includes basic research does not guarantee security; indeed, it tends to insecurity by insisting upon care where it is not needed and thus cheapening the value of care where it is vital. I would argue that we should clearly differentiate between basic research and technological development and have appropriate security measures for each. News items lead me to surmise that greater security may well be required in the case of technological development; but this should not imply that greater precaution is requisite also for basic research. On the contrary, I would argue that freedom is essential for basic research, and hence that greater security will be attained through the technological progress that will follow from complete freedom for basic research, rather than through confining, restricting administrative measures! Let me explain my reasons for these convictions.

In view of the unity of nature, it is not surprising that there is also a unity of science. Different points of view require us to have an increased communication, including the common language requisite for such communication—if we are to make maximum use of the findings of one another.

The increased specialization of scientists necessitates increased communication. We can substitute for the iron curtain a veil of security; but in shutting others out we must not forget that we are enclosing ourselves. In this respect, we are undoubtedly harming ourselves more than others. Prof. M. C. Vallarta, a member of the Atomic Energy Commission of Mexico, told me how amazed the audience was at the first meeting on atomic energy at Geneva a few years ago. Each of the nations had declassified some of its highly classified material. For the first time some of these facts were being presented to the world at large. An American drew a curve on the blackboard showing the relations between certain physical quantities; then an Englishman revealed the British findings—the curve was identical; finally, a Russian showed the Russian result—the curve was the same. Everyone was amazed. Each nation had the same information, which had been developed in each case behind a veil of secrecy.

During World War II, a colleague of mine was working on high explosives, such as TNT. None of us had occasion to be cleared for the Manhattan Project. One day, however, he wrote down some ideas he had as to how to produce an explosive using nuclear processes. His paper was turned over to Naval Officers. Imagine their consternation when they realized that he had written out essentially the basic idea of the Manhattan Project. The paper was immediately seized and highly classified. One cannot thus envelop men's minds in veils of security; thoughts are not too confined by any man-made barriers. One is reminded of the old story about the horse that was lost, and the man who found it. When asked the secret of his success, he replied, "I said to myself, 'If I were a horse, where would I go?' I went there, and there was the horse." Men's minds are much the same the world over. Occasionally, there is a unique genius, but given enough time the same idea will germinate elsewhere. The growth of an idea depends upon communal reception as well as upon pregnant conception. The history of science has shown again and again that individual advances are eventually overtaken by social advance.

As we review American history, we are conscious that the American genius has expressed itself more often in the applications of science, in the developments of technology, rather than in the creations of basic research. It would seem wise, therefore, for us to encourage free communication among scientists in basic research. If history repeats itself, the chances are that we will gain more than we will give. Under any circumstances, the availability of scientific knowledge is no indication as to how that knowledge will be used. It is the "how" that demands security classification necessarily—not the "what." Let us recall that atomic fission was discovered not in America, not in the NATO countries, but in Germany. Americans, however, realized its practical potential; they proceeded to develop this principle into usable atomic energy.

I would, therefore, argue strongly for complete freedom for all basic research. I would maintain that National Security will be enhanced by the very increasing of such freedom, that it might well be endangered by ignorant attempts to set up veils of security—we would probably be ensuring our own ignorance more than that of others! Mind you, I am speaking of basic research—not development—as the necessary foundation for our continuing technological progress.

Remarks of RICHARD ARENS, *General Counsel, House Un-American Activities Committee*

Mr. Chairman, I am not competent to observe whether or not this is a scientific age. On the basis of extensive experience at the heart of the anti-communist program of this government I feel I am competent to observe that this is an age of war—an age of total war—in which the Soviet Empire with thirty-three million agents on every continent of the globe, an empire of nine hundred million people, is at war,—a political war, economic war, yes, a scientific war and military war with the number one target the United States of America.

I think, too, Mr. Chairman, I am competent to say today that the Rosenbergs were not sent to the gas chamber because they were passing imagination, concepts, philosophical ideas. They were sent to the gas chamber as atomic spies because they were passing military secrets to the enemy of this nation which is now engaged in a total war on every front, within every field within the comprehension of the human mind, to destroy this nation.

This veil of secrecy concerning which our friend speaks is simply a veil between us—between our scientists, between our know-how and those of the enemy which would destroy us, an enemy which has in the course of just two decades stolen our atom bomb secrets, stolen much of our know-how and is now competing with us almost on a par in almost every area of the world. . . .

Legislation which would have precluded access to the defense facilities of communist agents, communist saboteurs was not passed by the United States Congress. It didn't pass the House Judiciary Committee, didn't pass the Senate Judiciary Committee, didn't pass either subcommittee, didn't even come in to vote. Why? Because political pressures were brought by the communist apparatus and by those who cannot perceive the threat, not of philosophers, not of men of imagination, but of communist agents now in our defense plants.

Over the course of the last generation United Electrical Workers has been exposed time and time again as controlled by communist agents. It was ejected from the CIO because the CIO found it was communist controlled, communist dominated. Right now while I am talking to you we on our staff can identify approximately forty plants in which UE, controlled by the communist conspiracy, has contracts in which they are working on defense facilities, including some facilities for the guided missile program, atomic energy facilities, and the like.

UE now is operating in over two hundred plants in this nation and it is an unfair labor practice in most instances for the employer to discharge the communist after he has been identified under oath by a live witness as a communist—not as a philosopher, not as one of imagination, but as one who would pass defense secrets to the enemy—the enemy which has on the basis of defense secrets passed to it risen to an ascendancy that now challenges the last remaining bulwark of freedom on this continent.

While I am talking to you right now the International Union of Mine, Mill & Smelter Workers has 65,000 members in the vital defense plants of this nation, and the International Union of Mine, Mill & Smelter Workers is controlled lock, stock, and barrel by the communist conspiracy. The top echelon has been identified time and time again by responsible witnesses under oath who lay their liberty on the line and identify them as communist saboteurs and Communists—not as philosophers, not as men of imagination, but as part and parcel of an international conspiracy that threatens to destroy us.

You tell me, Is it not in the public interest to cause this veil of secrecy, if it can be so created, if it can be fabricated to protect this nation from the dissemination of that information which may be available? I plead with you today to accept the minimum fact that communists are communists, that communism is communism, and that the Soviet empire is now at war with the United States of America.

If that seems in this audience to be rather naive, elementary, let me say that the Supreme Court of the United States has not yet accepted that fact in the Watkins case. The Supreme Court of the United States opened its opinion by saying—and this is almost a quotation—that a congressional committee may expose graft, waste, and inefficiency is unquestioned; but the congressional committee does not have power to expose political belief, political opinion, political activity. And then in the very next paragraph [the Supreme Court] equates communism, the communist conspiracy, and communist activity in these United States as political belief, political philosophy and political activity.

I say to you as one who has been at the heart of the anti-communist work of this Government for over a decade we need *more* security and not *less* security. We need more attention to the preservation of what secrets we do have remaining and not less. We need a greater offensive against the communist operation within this nation and not less. You say, "Oh, isn't everyone now today against communism and against communists?"

Am I just talking about something that everybody agrees to?

Let me just give you one or two illustrations which we could multiply ad infinitum. The field of education,—the field for which the eminent spokesman came and spoke just a moment ago—was identified before our committee (and this is just typical) by a live witness under oath, responsible, of integrity, a man by the name of Raymond Lavolli, as communist. Lavolli was then teaching at Dickenson College in Carlisle, Pennsylvania.

Lavolli was interrogated before our committee. "Are you now a member of the Communist Party?" Lavolli invoked the Fifth Amendment, as he had a right to do. Therefore a transcript of those proceedings was sent to Dickenson College at the request of the board of education. Lavolli was called before the board and dismissed. Thereafter, within two weeks time, the American Association of University Professors, representing assuredly the elite of intelligentsia of the nation, issued a blanket condemnation of Dickenson College for firing this communist on the ground that they are interfering somehow in thought, concepts, freedom of expression, and the like.

The security program of this government, let us never forget, is devised, [and] is in operation for the purpose of maintaining a security of this country against the encroachments of the international communist conspiracy which threatens free men everywhere.

Let me give you just one more illustration. You wonder why we in our work get just a little bit discouraged. The Congress of the United States, recognizing the fact that we are now not in a philosophical contest, not in a contest of ideas and imagination, but in a contest of survival, passed a law precluding trans-shipments of certain strategic materiels to the Red bloc.

On July 8, 1956, the Permanent Investigating Subcommittee of the Senate issued a report with this conclusion: Notwithstanding the law forbidding financial aid to allies which ship strategic materiel to communists, two hundred strategic materials have been removed from the list. I picked up out of the Washington Evening Star just a month ago, August 15, this article:

"The United States is reluctantly easing its curbs on trade with the Soviet bloc in Europe. It is doing so under pressure from allies and American businessmen in search of new markets. Included in this list are strategic materiels, strategic metals."

I say to you in my humble judgment that a dire prediction can be made; just as this scrap iron which went to Japan prior to its ignominious attack at Pearl Harbor came back in the bodies of our young men of this nation, so, too, if this course is pursued, unless we shake the cobwebs from our eyes and see the realities of the treachery that is about us, these metals which have been released for trans-shipment to the Red bloc will likewise return to America in the dead bodies of her youth.

I could not in this theme close without a quotation from a great American, J. Edgar Hoover. In recent words he said:

"Public apathy is the sure way to national suicide—the death of individual freedom. Public apathy enabled Hitler's Fifth Column to prepare Europe for each Nazi coup. Public apathy allowed the communists to penetrate and make satellites of once free countries and it is presently enabling them to honeycomb and weaken the structure of freedom in the remaining countries. And there is today a terrifying apathy on the part of Americans toward the deadliest danger which this nation has ever faced. Some of that apathy is deliberately induced by elements which desire you to believe that the Communist Party, USA, no longer represents a threat to America. You hear that domestic communism is reduced in numbers, that it is divided, split, shattered. You read the proclamations of well-meaning but uniformed indivduals who, from their mountain of ignorance, maintain Americans are too worried over domestic communism—that citizens who consider the 'misguided aberrations of a handful of persons' to be a danger to our security are mistaken.

"The Communist Party in the United States is not out of business, it is not dead, it is not even dormant. It is, however, well on its way to achieving its current objective which is to make you believe that it is shattered, ineffective and dying.

"When it has fully achieved this first objective it will then proceed inflexibly toward its final goal. Those who try to minimize its danger are either uninformed or they have a deadly ax to grind."

Remarks of DR. ELLIS A. JOHNSON, *Director, Operations Research Office, The Johns Hopkins University*

I had a reasonably long experience with security. I agree that there is a tremendous danger from communism, the greatest we have ever faced. There is a great danger from subversion and espionage. However, the problem is not the sterile one of security by itself or security as it can aid the United States over the long run as well as the short run in making us superior in military strength to the Soviet Union.

I am one of the young men—or relatively young at that time at any rate—who had this iron thrown back at us in the Pacific, but I had ten years in research, five years in weapon development before that. In Korea I saw the many innocent civilians killed by the Soviet communists. I would like to put some of these things in perspective, not security by itself but the development of technological superiority. We have to face our present situation.

Now, I agree with Dr. Seeger that in basic research you cannot really apply security successfully. There is a good reason. There are a hundred thousand technical journals putting out the dope every month, and this is a whirlpool of knowledge. Our contribution is relatively small out of the proportion, and if you do know the basic principles then you can apply this knowledge very successfully.

I have a story about the principle. There was a man who was producing whisky illegally in Maryland. The revenuers never caught him because when they came in they could not find anything to identify as a still. They were patient, and one day they

did. He was doing this with a garbage can, a three-legged kitchen stool, a wash basin, and a tumbler. He would put the mash in the garbage can, heat it up some, put the three-legged stool beside it, tilt the wash basin upside down, and put a cake of ice in it and the tumbler on the edge. He made very good whisky, serving himself and his neighbors. It was very easy to get rid of, and, if you do know the first principle, then there isn't only one single way of solving the problem. The communists know the first principles as well as we do. . . .

We have to accept the fact that security is not important in the state of basic research. The situation is very different as we get toward engineering, production, and use. Let's see where we are. We know that at the end of World War II we were four or five years ahead of the Soviet Union. We did things very fast. Dr. Karl Compton once noted that the old motto, "From research laboratory to freight car equals seven years" could well be changed to seven months for the World War II period. Now the question is, "What has happened since then?"

Atomic weapons, the favorite subject of security, is one that can be well spelled out. This has been covered in the presss. The United States tested its first A-bomb in 1945. We thought we had a monopoly. The Soviet Union tested its first A-bomb in 1949 and shocked the experts who thought the Russians incapable of achieving it until six years later. The first United States hydrogen bomb test came in 1952; the Soviet H-bomb test in 1953.

However, in carriers for such weapons the Russians have out-planned and out-produced us. They were first in an airdrop of an H-bomb; the Soviet Union in 1955 and the United States in 1956, and there were no stolen secrets here. Intercontinental jet bombers were in operation for both countries in the same year, in 1955. We have had a lot of scoops—the Nautilus, for example. However, in ballistic missiles we have been behind generally.

The Russians tested a motor in 1951 for a projected intermediate range missile. They had faith that they could package a small H-bomb. We waited for the bomb before starting the missile. Then, logically enough, the Soviet Union's IRBM's were reported operational in 1955. It has been estimated that the Soviet Union in 1958 has a stockpile of 500 ICBM's, though other reports indicate this is out of bounds, when our ICBM distance requirements are imposed.

The Soviet designations for both IRBM and ICBM include lower ranges than the United States designations. One estimate credits the Soviet Union with 100 ICBM's against 30 for the United States in 1960, and 2,000 for the Soviet Union against 120 for the United States in 1964.

Now that is one story. You could find a variety of patterns in the press if you wanted to pick just the statistics and perhaps prove anything. You may feel this is true of press reports in general. The significant point is, and I doubt that you will argue, that the United States had a minimum lead of four years in 1945, as the Senate Preparedness Committee concluded on the basis of the evidence of all of the noted leaders of World War II, ranging from Vannevar Bush to Nimitz, Marshall, and many others. Today the Soviets have a better balance in weapons and carriers than the United States, according to the testimony of present leaders, again of the Senate Preparedness Committee and to the Robertson Committee. The United States' lag in technological development makes us now face the dire years of the much discussed missile gap in the period 1960-1964.

The catastrophe in the situation is that the Soviet Union is getting where it wants to go faster than we are getting where we have to be. The Robertson Committee; William Foster, the Chairman of the Gaither Committee; General Gavin; Admiral Rickover, and others agree with me that the Soviet Union's lead time in weapons development is now about half the United States lead time. This, as you well know, portends ill for the future.

The Soviet Union has adopted the procedures that proved effective for short lead times in the United States during World War II, while we have extended lead time to perhaps four times our World War II lead time. I estimate the approximate average lead time of United States weapons systems from concept to operational capability to be ten years at the present time, that of the Soviet Union, five years. These, I believe, are credible estimates.

For example, last year the Soviets revealed the TU-110 military-civilian jet transport that is reported to have been designed, built, and flown in eighteen months. That is mighty fast work by any standards, although we did it just as well—in fact, better—during World War II. The Robertson Committee's official analysis, also in 1957, identified an average of eleven years for United States lead time in military aircraft.

There are many factors involved in this stretch-out: lack of hot war urgency, ineffective planning, few if any timely decisions, sloppy organization, and so forth. One important one, I feel, is the restriction on communication resulting from the need-to-know security regulation.

Now I believe in our concepts and I believe them practical—even strengthened personnel security. Following Dr. Seeger's argument, there is a requirement for unity and complete knowledge within the security system because we surely ought to be able to avoid inside security which hinders our technical progress. If we can only find some way of getting secure personnel and secure organizations, then we can remedy some of our long lead time by changing our situation and need to know.

Dr. Berkner, well acquainted personally with government security regulations and their effects, has estimated that ninety per cent of the scientific and technical information could be made public because the Russians know it, the principle,—as well as ourselves. But that is a separate argument. The need-to-know concept is the immediate point of concern.

The need-to-know concept has been written into United States military regulations for over a hundred years. In the beginning it applied to troop movement

and troop dispositions. Today the military's need-to-know regulation applies to all classified defense information. This is the stumbling block in research communications.

In the Soviet Union, research is centralized. The channels for obtaining information are open to all who do need to know. In the United States, military research is spread throughout the services, industry, and the universities. We apply the need-to-know rule separately to each and every individual involved in military research and development and such application restricts the individual pretty much to his own small working group in the Army, Navy, Air Force, or contract unit.

So it is that not only individuals can't talk to persons in related research, but Army or Navy groups are restricted in talking to Air Force groups working on the same or similar problems.

The testimony before the House Government Information Subcommittee over a two-year period spelled out the research losses resulting from such rigid security controls with respect to the need to know. In April of this year the committee's view was that "the only real national security lies in scientific progress" and that "scientific progress relies on a free exchange of ideas." It was based on the general concept that "in the area of research and development, knowledge and need for it walk hand in hand."

C. C. Furnas, former Assistant Secretary of Defense for Research and Development, is among those who have advised knocking out the need-to-know barrier.

Striking the need-to-know control from research and development is perfectly feasible. Subsequent to the hearings Chairman Moss stated that changes in the security program could be made by the Congress but that this method would be difficult and slow. He pointed out that the revision should be made through administrative action or through a coordinated program recommended to the Congress by the Executive.

Most creative weapons systems research is done by American industry. Need-to-know limitations make it almost impossible for industry to get access to the information necessary for it to do a good job for defense. Industry cannot get adequate classified information until it has a contract, and it cannot establish the basis for a contract until it has adequate classified information. We must break this vicious circle if "no contract, no need-to-know; no need-to-know, no contract."

I inspected the classified library of one company deeply engaged in work for defense. Working at a level of about $200,000,000 a year this company has two classified librarians and a meager 10 by 20 storage space for classified documents. Upon investigation I discovered that the fault was not the company's, but the Department of Defense. I knew of literally hundreds of classified documents they required, but are denied on a need-to-know criteria. They needed to make the $200,000,000 a year in order to effectively use the company's money in development. That company actually needs about forty classified librarians and a classified document to go along with it and a full set of the other things that are needed if you are going to communicate all of the essential facts to the people that are going to cooperate.

To summarize I will quote the report of the Senate Preparedness Subcommittee, chaired by Senator Lyndon Johnson:

> *"On the basis of sworn testimony by top scientists, leading industrialists and government and military officials, it can now be said:*
>
> *"(1) The Soviet Union leads the United States in the development of ballistic missiles.*
>
> *"(2) The Soviet Union leads the United States in number of submarines, which raises the possibility of attack with modern weapons or missiles, although, the indications are that we are ahead in the production of atomic submarines.*
>
> *"(3) The Soviet Union is rapidly closing the gap in manned airpower and, at present rates will surpass this country in comparatively short time.*
>
> *"(4) The Soviet Union has a system which enables it to develop new weapons in substantially less time than the United States.*
>
> *"(5) The Soviet Union has led the world into outer space.*
>
> *"(6) The Soviet Union is producing scientists and technicians at a rate substantially greater than our country."*

I would say to Lyndon Johnson, "You can improve this situation, potentially fatal to the United States, more by a tremendous liberalization of the need-to-know to trusted individuals and organizations who have appropriate personnel clearance than by any other single action."

The existing policies on need-to-know are at the minimum stupid and at the maximum criminal, if we want to speed up United States military development. Let us tighten up personnel security and greatly liberalize need-to-know policies in order to restore our vanished technological supremacy in defense.

BE SURE TO ATTEND THE . . . .

American Society for Industrial Security 1959 Convention/Seminar

Ambassador Hotel, Los Angeles, California

September 21-23, 1959

WORKSHOP/SEMINAR I

PHYSICAL SECURITY PLANNING, By JOHN G. SEARLE, *Industrial Security Specialist, Office of the Assistant Chief of Staff, G-2, U. S. Army*

Physical Security Planning—this topic does cover a myriad of jobs, conditions and headaches for the person or persons charged with the reponsibilities of the planning. Open for consideration in this field—and some of the few things to be taken into account will be: security from "acts of God"—storms, floods, lightning, earthquakes, etc—and security from "acts of man"—sabotage, espionage, theft, arson, accidents, war damage, civil strife, strikes, etc.

Not the least of things to be considered will be the financial and physical means for the repair and restoration.

Obviously all facets of such a planning program cannot be covered here, so we will discuss one facet of the Physical Security Planning program. Specifically, Physical Security Planning as it pertains to the safeguarding of classified defense information in the performance and execution of classified defense contracts. Speaking in very general terms "security" in this instance can be broken into three categories: (1) Physical Security, (2) Document Security and (3) Personnel Security. These three categories are very closely inter-dependent and inter-related and each must be fully planned and fully implemented to achieve a bare minimum of satisfactory security.

Before solving any problem, the problem must first be stated. In this instance we have an industrial facility or firm that must plan, install, and implement all physical safeguards required to adequately store, protect and safeguard classified defense information in compliance with contractual and statutory requirements. Very briefly, these requirements are as follows: "To deny access and/or opportunity for access, by sight and sound, to all persons who are *not* cleared and to all persons who do *not* have a specific "need-to-know" in the performance of the specific classsified contract concerned."

Under the Industrial Security Program of the Department of Defense each industrial security facility will have a security cognizant office under the Department of the Army, Department of the Navy or the Department of the Air Force. This office will be charged with the responsibility of supervising the Industrial Security Program and providing necessary guidance and assistance in meeting all security requirements.

Prior to the issuance of a Facility Security Clearance the cognizant security office is required to conduct a Facility Security Clearance Survey. During this survey, a representative of the government will be present at the facility to determine if existing safeguards are adequate or, if not, what additional safeguards will be required. It is desirable and to the facility's advantage to prepare in advance for the conduct of the Facility Security Clearance Survey, but at this point up jumps the devil in the form of the question: "What will be required and where can we find the requirements?"

The bible on security in this instance is contained in two basic documents. First, The Department of Defense Security Agreement, (DD Form 441) and second, The Industrial Security Manual for Safeguarding Classified Defense Information, (Attachment to DD Form 441). These two documents set forth the contractual security requirements and paragraph 2, Section I of the Industrial Security Manual lists the "Applicable Federal Statutes and Executive Orders," which in turn set forth the statutory security requirements.

In addition to these two documents the contracting officer of the government procurement agency is required to furnish both the facility concerned and the cognizant security office concerned, a copy of the Department of Defense Security Requirements Check List, (DD Form 254). The Security Requirements Check List sets forth detailed requirements for the specific contract and, where applicable, any security requirements that are in excess of those contained in the Security Agreement and/or the Industrial Security Manual.

To begin, the planner or the planners will require a thorough knowledge of the following:

a. *THE FACILITY*:

(1) geographical location and physical arrangement, (2) operational methods, policies, and procedures, (3) methods of shipment or transmission of the end products, (4) methods of shipment or transmission of source or raw materials, (5) capabilities and limitations of the facility's means of production, (6) capabilities and limitations for expansion, (7) personnel procurement policies and capabilities.

b. *THE CONTRACT*:

(1) What is the job? (2) Time limitations, (3) Cost limitations.

c. *SECURITY REQUIREMENTS*:

(1) requirements outlined in the Security Agreement, (2) requirements outlined in the Industrial Security Manual, (3) requirements outlined in the Security Requirements Check List, (4) security requirements imposed by management.

d. *PHYSICAL SECURITY METHODS*:

(1) physical barriers—fences, gates, doors, locks and locking devices, windows, walls, roofs and bars and grills; (2) Supervision of Physical Barriers— guards, alarm systems, inspections and security education; (3) "Open," "Restricted" and "Closed" Areas—requirements, locations, segregation, controls, personnel identification and security education; (4) Classified Containers—vaults, safes, file cabinets,

locks and locking devices, combinations, changing of combinations, protection of combinations, dissemination of combinations, inspections and security education.

After becoming familiar with these basic items the planner can begin a physical security survey. This survey should be conducted to determine the specifics in superimposing a physical security program upon an established plant or upon a plant to be constructed. It might be well at this point to interject that the planners have two jobs. One, to provide for the physical security of classified information and, secondly, to provide sufficient latitude in the security requirements for the actual execution aand performance of the contract.

Physical Security Planning cannot be divorced from document and personnel security in any stage of a program. There are seven basic safeguards which, when properly implemented, will provide good security within any facility:

(1) Thorough indoctrination of personnel;
(2) Limiting access to those who "need-to-know,"
(3) Proper clearance of individuals prior to access;
(4) Maintenance of proper custody;
(5) Adherence to marking and handling requirements;
(6) Appropriate disposition and/or destruction;
(7) Adherence to proper procedures prior to release.

Use these keys in your planning; they are the foundations of "security."

SABOTAGE—METHODS AND TARGETS, By FRANK A. KNIGHT, *Chesapeake and Potomac Telephone Company*

Public interest today is centered upon man's efforts to conquer space and upon the intense rivalry between nations to develop more powerful atomic weapons. Most of us have been thrilled, no doubt, with announcements of the successful launching of our space satellites. And current reports about our new developments in the fields of inter-continental guided missiles and jet-propelled aircraft are met with counterclaims of greater accomplishments by our world adversaries in the international armament race.

These major events in the pattern of national defense and scientific exploration may, however, be blinding many of us to the ever-present dangers of industrial sabotage. We all know too well that a coordinated sabotage effort directed at our great industrial potential in this country would result should the "cold war" develop into a shooting conflict.

I have no reason to minimize the catastrophic results of successful enemy attacks using any of the mass destruction media well known to all of us. However, the relative simplicity of sabotage methods at the outbreak of hostilities, coupled with direct enemy attacks on our large cities and important industrial centers, would indicate that sabotage can be anticipated in any plan of attack.

Sabotage makes itself felt in various ways and at vulnerable points in our industrial structure. . . . . sabotage is "the malicious disruption, or attempted disruption, of the normal functions of a nation in any manner which intends, or apparently intends, to hinder the defense production or its potential therefore."

Now let's examine the subject. Who is our adversary? What is he like? How does he operate? There are generally two types of sabotage agents. One is the independent or individualist as contrasted with the enemy agent under the direction of a foreign government. The independent or individual saboteur has no direct connection with a foreign government or military group. Yet his overt acts of omission and commission come under the heading of sabotage as surely as if he were in the employ of a hostile government. There are many reasons we can think of for his actions. He holds a grudge against management or his immediate boss; he wishes to gain personal attention; he believes what he does is performed out of sympathy for a foreign people or government, or for any number of less definitive reasons. The independent agent is dangerous because his actions can seldom be predicted or anticipated with any degree of accuracy. He often acts on impulse and has no coordinated or integrated plan. However, because his acts have no coordination, the over-all effect on the war or defense effort is not felt as much as that of a directed enemy agent or group of agents.

The enemy agent in the employ of a foreign government is the more dangerous saboteur. He is directed, trained, supported and supplied by a skilled group or sabotage organization and his efforts are coordinated into the over-all effort to impede and disrupt our industrial potential. Sometimes agents work alone, but in other instances they operate in small groups. Biding their time, they may remain hidden for months or years and then, at a given signal, commit one or two major acts of sabotage and will fulfill their entire mission and justify their existence. Naturally, this makes it extremely difficult to combat this kind of operation.

It is not always necessary for a saboteur to achieve complete destruction of his objective to fully accomplish his mission. Often partial destruction, panic or confusion will suffice. There are two things the sabotage agent usually has working for him, namely, the element of surprise—he picks the time, place and target; and the element of camouflage—he often can cause the act itself to appear accidental or natural.

I would like to discuss briefly some of the ways in which a saboteur might accomplish his mission. First, there is fire. The use of incendiaries to commit sabotage has many advantages. Its successful use tends to hide its true origin since fire is a natural hazard in many industries and does not necessarily raise suspicion of sabotage. The tools for sabotage by fire are simple and generally are readily available at the target site. There have been several manuals published on this subject by the armed forces and

fire insurance companies which are available to you so I shall not burden you with any detailed examples of this type.

Secondly, there is the use of explosives. When the target itself is known to be fire resistant the enemy agent must consider the use of a more positive means to accomplish his objectives. In some industries and at some facilities, explosives are normally used or stored in relatively large amounts. Such a condition would be expected to provide the proper camouflage for a saboteur bent on using explosives. On some occasions the agent may wish to affect employee morale or public opinion. Certainly a small smoke bomb thrown into a crowded plant cafeteria during the lunch hour might not hurt too many people, but it could affect employee morale adversely and cause some disruption of production at the plant for awhile.

Thirdly, there is sabotage by mechanical means. This category affords a potential for the greatest number of individual incidents in industry. Mechanical sabotage is most effective when employed over a comparatively long period of time. It generally involves a large number of individual acts carried out on a coordinated basis by a large group of people.

There are six subdivisions of mechanical sabotage which I shall discuss here in some detail since our interest and responsibilities are to be found in this field more so than in the first two categories. These six types of mechanical sabotage are: breakage, acts of omission, substitution, contamination, use of abrasives, and electrical interference.

The first type is the simple act of breakage. Was it deliberate? Was it accidental? Who is to say? Was it done with intent? If so, was it sabotage? Perhaps, but to prove it is a most difficult matter.

Let us consider the act of omission. It involves the failure to do those things which are normally expected of workers on the job, such as, failure to tighten key bolts; failure to gauge properly, or failure to provide the proper lubrication. Undetected, such acts may result in damage on a large scale to finished products. On the other hand, workmen whose acts of omission are detected may alibi in many ways and blame it on forgetfulness, personal problems, lack of training, etc.

Sabotage by substitution frequently results from the use of an inferior part or component in place of the correct part in an assembly. This action could cause a breakdown or result in undue wear, which in turn, would cause interruptions in production. Again, spurious orders might be substituted for official directives thereby causing confusion, delay and endless work in tracing lost shipments.

An example of this kind of operation comes to mind here. During World War II, Allied agents altered railroad freight waybill destinations on war supplies intended for shipment to German army units. The German high command eventually found whole train loads of material direly needed on the eastern front at locations in southern France or on the Italian border. Yes, substitution is quite simple and often very effective.

Contamination is another type of mechanical sabotage. It often requires a minimum of effort and may take the form of introducing gas into the ventilating system of a plant or large public building. Foodstuffs such as sugar, butter or cheese can be made unfit for human consumption by use of kerosene, sand and other foreign substances.

The use of abrasives in the hands of a saboteur can easily cause excessive damage and delay. The use of such agents as emery dust, metal filings or sand thrown on fast-moving or highly-polished bearings or parts will cause undue wear, overheating and eventual breakdown. This type of overt act is also effective and difficult to combat.

Electrical interference with or interruption of electric power, telecommunications, radio and radar systems is another kind of sabotage with which all of us are familiar.

The fourth major category is psychological sabotage. This deals with the fomentation of strikes, jurisdictional disputes and unrest; inducing excessive spoilage and inferior work causing a slowdown of operations, or, on a broad scale disseminating inflammatory propaganda in order to break down morale in the target industry or organization.

Sabotage, as I have stated earlier, is generally a coordinated effort directed at targets which are quite carefully selected. Each target is measured against four basic criteria: first, for its effect on the war or defense effort; second, the accessibility of the target to an agent; third, the method or destruction required, and, fourth, the replacement factor together with its time element.

Let's take a look at some potential targets of saboteurs. In 1947 a complete sabotage survey of every major industrial center in these United States was made by Communist Party sabotage squads. In 1948 and periodically on a continuing basis the communists have made elaborate re-checks of the previous years' surveys. In these cases the analysis concentrated on the spotting of industries and facilities that hold a key position in our national defense posture. Communications and transportation centers were emphasized. This re-review of their basic plan, considered whether it would be best to sabotage a series of plants where a particular finished product is turned out whether it would be more effective to side-track all of them by crippling instead the single subordinate facility that supplies those plants with vital raw material and or parts.

A number of people would have us believe that sabotage is something that takes place only during wartime. I would like to quote a case which was reported in a number of newspapers on June 10, 1954, which certainly belies such a fact.

> *"Saboteurs have ruined* 1000 *electric capacitors manufactured by the Hopkins Engineering Company here for Navy radar sets, city detectives said today.*
>
> *"Ralph E. Strahl, Executive Engineer of the firm, told detective Frank Repetti and Don Rodman last night that if the wrecked electronic parts had been placed in radar sets they could have caused great damage. Strahl explained to*

the officers that salt had been sprinkled into two cartons containing 500 capacitors each. The capacitors are so sensitive that any contact with salt renders them inoperative. Officers said that the use of salt to damage the capacitors indicates the sabotage was done by someone familiar with their construction."

What can we do to prevent sabotage?

First of all, watch for the individual who pretends to be a loyal worker, who is industrious on the job, who shows interest in the work of others and avoids remarks betraying enemy sympathies, but who learns all he can about the layout of the plant or office, unguarded vulnerable spots and the habits of plant or office personnel.

Next, watch for the individual who fouls up production by making fractional errors on precision instruments, by loosening bolts in vital sockets, or by creating small bottlenecks that delay major projects.

Third, watch for the individual who seizes any opening to weaken morale by capitalizing on grievances, encouraging malingerers, and feeding dissatisfaction.

Fourth, watch the individual who waits for his chance to instigate major strikes, destroy machines and equipment, demolish important structures, and injure key personnel.

The saboteur can be combated by a careful inspection of all equipment, frequent checkup on physical safeguards, and by watching for "kinks" all along the line. He can be confined in close quarters by constantly guarding valuable equipment, providing foolproof storage for valuable documents, denying admittance of unauthorized persons to restricted areas, and by keeping an eye on every unidentified person.

He can be defeated if you move fast to report defects to proper authorities and reinforce weak spots in your area.

DETECTION OF SABOTAGE EFFORTS, By JAMES C. LYNCH, *Redstone Arsenal*

I will endeavor to cover the efforts that you as security officers should make in order to prevent sabotage. This should be accomplished through a concerted effort by military commanders, the management of civilian installations, intelligence personnel, physical security personnel, safety personnel, fire inspectors and fire fighters, and persons who employ and assign civilian and military personnel. Security measures may include the following:

a. Screening, investigating and re-investigating all personnel having access to the installation in order to prevent the hiring, assignment and continued employment of disloyal, disgruntled and unreliable persons.
b. Instituting means and procedures to positively and rapidly identify persons entering or leaving the installation or facility.
c. Guarding the perimeter and entrances of an installation to exclude unauthorized persons and potential sabotage material.
d. Guarding and maintaining surveillance over the interior areas of the facility especially when the plant or installation is not in operation, that is, at night or over the weekend.
e. Restricting entry into sensitive or classified areas or facilities inside the installation.
f. Safeguarding classified information to deprive potential saboteurs of facts they need to plan and execute sabotage.
g. Instituting measures and procedures to control the storage, possession and use of dangerous materials inside the installation.
h. Examining materials and supplies delivered to the installation as well as the delivery vehicles or conveyances used in order to insure that sabotage materials are not brought into the installation.
i. Stationing guards and installing lights and warning devices at key sensitive, critical or vulnerable facilities at the installation.
j. Investigating security violations and suspicious incidents to establish cause, intent and personal responsibility or involvement.
k. Excluding persons of criminal or questionable character and maintaining a realistic law enforcement and crime prevention program.
l. Conducting frequent and thorough crime, security and safety surveys and consistently executing corrective measures.
m. Educating personnel to make them "security conscious" and alert to the sabotage threat. (Training in security should strive to encourage employees to cooperate with security personnel voluntarily, comply with regulation and promptly report any suspicious incidents.)
n. A concerted and consistent effort by all concerned to achieve and maintain high morale and efficiency among employees of the facility.
o. Striving continually to insure that the premises, facilities and equipment are kept clean, orderly and in good repair.
p. Preparing and planning to meet emergencies that might interrupt operations, hamper guard force activities, or present opportunities for saboteurs. Such planning must provide for:
   (1) Evacuation from threatened or damaged areas.
   (2) Means and procedures to permit the rapid notification, identification, and free movement of personnel engaged in duties such as police and security evacuation, rescue and salvage, fire fighting, decontamination and bomb disposal.
   (3) A supplemental guarding of vital facilities subject to sabotage.
   (4) The control of damage areas and the protection of evidence and property.
   (5) Fire and damage control.
   (6) Traffic control on key routes and at key intersections.
   (7) Reliable communication means and procedures
   (8) The direction and coordination of emergency measures.

Your responsibility is to organize and train volutary auxiliary personnel from civilian workers at your plants or military installations in order to increase normal protection against sabotage and to provide added physical security personnel during emergencies.

I will endeavor now to discuss some of the investigative efforts which must be accomplished in a suspected sabotage. Sabotage investigation within military installations are the responsibility of the Counterintelligence Corps whereas the Federal Bu-

reau of Investigation handles such cases in most industrial facilities. Military Police do not conduct sabotage investigations, but will confine their activities to the prevention of, and defense against, this security hazard.

When an incident appears to be actual or suspected sabotage the scene will be isolated and the local staff intelligence officer will be immediately notified. When a suspected or actual sabotage incident occurs within an industrial facility, the FBI should be immediately notified. A successful sabotage investigation depends largely upon the rapidity with which the appropriate investigative agency is notified.

A sabotage device is often the best evidence for the investigator as well as the source of danger to the person tampering with same. When any person finds an object which he believes to be a sabotage device, it is imperative that the following steps be taken immediately:

a. Evacuate the area at once if the device appears to be of an explosive nature, otherwise isolate the immediate vicinity.

b. Call the nearest Ordnance Officer and request that an explosives demolition expert rush to the scene. An engineer should be requested if it is a mechanical device. If the device is found at an industrial facility rather than a military installation, the FBI should be notifed and a similar request made.

c. Under no circumstances should unqualified personnel tamper with the device.

Those of you who have problems along these lines should analyze your installation or industrial facility with respect to the various protective measures which should be instituted in order to prevent sabotage. Toward that end, an outline, "Handbook on Physical Security," which is used in the Provost Marshal General School, might prove helpful. The school representatives at Camp Gordon, Georgia, who prepared the outline cover the following points:

a. External.
   (1) Your perimeter barriers covering fencing, openings, lighting, alarms and clear zones.
   (2) Your identification system which covers personnel, vehicles and material.

b. Internal hazards:
   (1) Your critical areas: (a) designations, and (b) control of these areas.
   (2) Movement: (a) personnel, and (b) vehicular.
   (3) Lighting.
   (4) Identification: (a) personnel, (b) vehicular, and (c) restricted areas.
   (5) Your guard force: (a) patrols, (b) fixed posts, (c) instructions, (d) training and (e) communications.
   (6) Your power supply.
   (7) Transportation.

To conclude I might recommend that those of you who haven't seen the television show, "Forbidden Area" which appeared on Playhouse 90, should do so. Prints of this show were made by the Air Force. Patterned after a book by Mr. Pat Frank, this television play depicts five Russian agents landing on the east coast of Florida, establishing residence in various sections of the United States, actually enlisting in the Air Force, obtaining positions with Strategic Air Command and conducting sabotage against B52 bombers by use of pressure bombs. These bombs, implaced in coffee thermos jugs, were taken up by the various crews and, after the plane reached a certain elevation, the bombs exploded.

This particular TV film would serve as a very adequate training aid in your security program.

The only sure way to eliminate the dangers of sabotage is to have a worthwhile protection program.

WORKSHOP/SEMINAR III

FUNCTIONS OF INDUSTRIAL GUARDS AND THEIR TRAINING, By JOSEPH L. DRISKELL, EPM, *Office of The Chief of Engineers, Department of the Army*

PART I: FUNCTIONS OF GUARDS

Under this topic we consider the functions of a guard force which is composed of specially selected and well-qualified individuals. Who (a) are hired as guards, (b) are paid guard wages, (c) perform duties of full-time guards, (d) are identified, or uniformed as guards and (e) are equipped or armed to properly perform guard duties.

The guard force is organized and utilized by individuals, corporations and governmental agencies to physically protect or secure the plant personnel, property or materials, prevent crimes and to enforce order. In other words, it operates "to keep what you have so that you can use it when you want it."

The degree of physical security applied to a facility, or a portion of it, is dependent upon the relative criticality and relative vulnerability of it.

Relative criticality of a facility, or portion of it is the impact that complete or partial loss would have on its ability to provide continuity of products or service. It is the importance of the whole facility to the big organizational element, or to National Defense.

Relative vulnerability is the probability of damage by possible means to a part of the facility, or the entire facility. This principle of "probability of damage" can be applied to big corporations and to National Defense.

Each of you have no doubt observed the guard functions at facilities other than your own and have recognized some of the elements necessary for an economical physical security operation which is also effective and efficient. Some of these elements are: (a) individuals, (b) barriers, (c) devices, , (d) sup-

port services (communications, transportation, fiscal, administration and others) and (e) management interest and support.

Of all of these elements, individuals—who can act, talk and think—are the most vital! They control the movement of persons, materials and all types of transportation.

Analysis of these three general responsibilities reveal the detailed functions, the primary missions, of a guard force which are to: (a) enforce personnel identification and movement restrictions; (b) apprehend persons and vehicles; (c) escort persons and vehicles; (d) patrol the facility; (e) check designated things, places and areas; (f) prevent crimes, incidents, accidents and fires; (g) respond to alarms and signals; (h) act properly in situations affecting the security of the facility; (i) investigate incidents and (j) write reports.

These functions, with local adaption are considered basic and normal functions of the guard force.

Your guard force is the most distinctive element of your facility. It is composed of selected individuals who possess valuable professional experience and training. Each member is a personal representative and salesman of the firm. He holds a position of dignity, prestige, great trust and grave responsibility.

The costs of the guard force amount to a considerable sum in the annual budget. Each individual represents a big personal investment. Accordingly the capabilities and professional talents of each member of the guard force should be diligently applied to the primary functions of the force.

Close observation of the duties imposed on each individual guard often reveals that he has "additional assigned tasks." These have been passed to the guard force because it is such an easy procedure and very convenient way to meet the requirement. Seldom can a guard or guard force assume "additional tasks" without jeopardizing the full and proper execution of their primary mission.

When these "additional tasks" prevail, the physical security of the facility becomes secondary. This is detrimental to the firm, the force, and the individual!

"Additional tasks" which reduce the effectiveness of the guard force, are menial in nature, and are degrading to the individual are; for example: (a) administrative switchboard operator for the facility after regular working hours, (b) custodial and janitorial duties, (c) helper in transportation pool between regular patrols, (d) driver of late-evening mail truck to adjacent city post office, (e) fireman of boilers and furnaces during regular and as well as after regular working hours and (f) administrative clerk in guard office.

When these and similar "additional tasks" are imposed on the guard force the situation can be easily remedied. All it requires is recognition that these "tasks" have to be performed, that they are not proper functions of the guard force and that other persons are available, and have the time to do these tasks if their work hours are adjusted to the needs.

PART II: TRAINING OF INDUSTRIAL GUARDS

In order for the guards to properly execute each of their functions, and be effective in their performance, they require special training.

Guards, at the time of employment, receive a basic type of training designed to establish and maintain high standards in the application of principles and techniques in the execution of their functions.

This basic training must be realistic, thorough, and aimed at developing:

(a) individual proficiency in security-type specialties, (b) effective integration of the individual into the guard force and (c) efficient guard force operations in the teamwork of the facility.

Aids should be used throughout all training including charts, maps, mock-ups, dummy or practice materials, and demonstrations. Individual participation in each training problem will permit evaluation of the student and an estimate of his potential. Oral and written expressions by the student cultivate confidence and aid him in doing a better job for the firm. Each student should be graded on each block of instruction, as well as on the complete course. A qualifying over-all grade for the course should be established. Competition among class members should be developed.

Subjects appropriate for inclusion in the training program of newly employed industrial guards are:

1. History of the firm.
2. The security program of the facility. Reasons for this program. Geographical area and location of the facility. Special or unusual conditions of the facility.
3. The guard force—its organization, mission and personnel.
4. Authority and jurisdiction—arrests, search, seizure and emergency actions.
5. Functions of guards: to support the guard force mission—preserve order; prevent accidents, incidents and crimes; control movement of individuals and traffic; promote public relations; act in emergencies and disasters (natural and nuclear); protect the facility, personnel, and property; cooperate with Civil Defense and other agencies.
6. Standing operating procedures in regard to handling minor and serious incidents, interviews and interrogations, methods of arrests, use of force, use of weapons, courtesy and respect, the traffic code, describing and observing persons, and protecting the accident or crime scene.
7. Reports and reporting procedures, including purpose and use of reports, important elements in a report, writing of reports, telephone procedure, radio procedure, and the necessity for security in all communications.
8. Instruction regarding weapons, including description, care, use and safety precautions.
9. Safety, first aid and fire prevention measures.
10. Vehicle care, operation and maintenance.
11. Self-defense (or unarmed defense).
12. Conduct and appearance.

Training on the job of a refresher nature is required on a continuing basis in order to maintain high stand-

ards of individual competence. This instruction should also be given as a class unit, scheduled in advance at regular intervals and not combined with regular duty.

Subjects for this instruction should include:

(a) Examples of outstanding as well as poor performance from which a lesson can be learned.

(b) Explain changes in policy and procedure.

(c) Emphasize conduct, appearance and courtesy.

(d) Discuss topics in which direct observation has revealed deficiencies.

(e) Test the individual on selected subjects to assure his professional knowledge.

(f) Hold practice exercises for actions in emergencies and disasters.

It is mandatory that the learning material be presented by qualified individuals who are good instructors.

The guard force, possessing capabilities essential to the physical security of the facility should be utilized in a manner appropriate to its outstanding professional qualifications and in conformity with its high position of trust and responsibility.

THE GUARD FORCE, AS EMPLOYEES, By TED D. TRACKLER, *Aluminum Company of America*

In a well managed plant, one of the first and certainly the most important steps taken toward establishing a good organization is the proper selection of personnel for all departments. A good selection program is always well planned and should include basic minimum requirements insofar as mental, physical and age limitations are concerned. Closely related to employee selection are adequate training methods designed to help employees to more readily become fully acquainted with company policies and procedures.

As one means of maintaining a currently efficient program, up-to-date standards of performance and job expectancies should be established, followed by regular periodical job appraisals. Management personnel can in this manner stay abreast of an employee's status on his job. Obviously, this mutual exchange of information is very beneficial to all concerned.

Through the selection procedures mentioned above, the company, in the beginning, has a good opportunity to check into the personal history and work background of each person employed, regardless of his job assignment. These methods will also provide the opportunity of hiring those people most stable, thereby considerably reducing the problem of manpower turnover. Anyone who hires and supervises guards knows the importance of having them constantly in the position of becoming thoroughly familiar with conditions in and around company plants and offices. . . .

It has become rather common practice for most industrial concerns to furnish and maintain their guards' uniforms.

To be better assured of quality workmanship, the guards' pay rates and take-home pay must bear a fair relationship to rates paid by industry for similar work in the plant area.

Training programs for plant protection personnel are of necessity built around the requirements of the operations involved, the kind of people who might be employed at a given location and in accordance with any additional requirements of the plant. Security agreements, location, climatic conditions and many other factors must be given due consideration. The very nature of plant protection work makes it essential that the guards be adequately trained to be thoroughly familiar with, and able to work under, these varied conditions.

Closely associated with a plant location, its people and the community, is the factor of having guards competent to handle their phase of public relations work. As has been said many times, the guard is usually the first contact the outside public has with the company and, this contact, be it good or bad, usually leaves a lasting impression. . . . While the public relations work of guards is much better in most companies than it was a decade ago, there is still considerable room for improvement, A good public relations attitude is generally stimulated by an employee's genuine interest in his company.

In addition to being thoroughly familiar with company rules, regulations, and policies, each guard, to adequately carry out his assignments, should also have a well-rounded knowledge of municipal, state and federal rules as they affect his particular duties . . .
Maintaining a good working relationship with local law enforcement agencies is a natural part of a day's work for an efficient guard.

Through day-to-day association, the alert company guards will become acquainted with employees throughout the plant and should gradually learn to know who the "characters" are and who the more stable and trustworthy employees are. Persons experienced in the field of plant protection are fully aware of the value of maintaining good contacts with people throughout the plant. These contacts can be particularly valuable when conducting investigations and when establishing and expediting theft control programs.

The guard who "grows up" and stays with the company will normally become thoroughly familiar

with the various aids to plant protection employed by the company. These may include employee contacts, close working relationship with the accounting and stores departments, mechanical alarm systems and any special procedures which might be necessary to solve problems in this phase of plant protection work. The same would apply to perimeter protection of the plant, including such things as power substations, pump houses, storage areas, waterfront and other areas requiring special attention.

Clock-watch patrols are usually laid out in a manner that will provide maximum coverage on foot or by motorized patrols with a minimum of effort and expense. It is customary to have the guards *become thoroughly familiar* with *normal* plant activities in order that they will readily recognize *abnormal* activities. When performing patrol duties, a guard must be well enough acquainted with his surroundings to keep all his five senses at work and employ a six sense —in this instance, memory. In these situations more than any other, it is highly essential that members of the plant protection force be kept up-to-date relative to changes of procedure.

When discussing plant protection operations with representatives of other companies, a standard complaint seems to be that guards are seldom adequately trained to prepare clear and concise reports. When planning training programs, it is very important that terms common to the operation of the plant be used freely. Well-planned report forms will serve as a guide to the guard, resulting in the furnishing of information necessary to provide good communications between the plant protection force and other members of management. It is recommended that newspapermen's routine of who, what, when, where and how serve as a basis for complete reports.

It is not uncommon for the plant guard to be an integral part of the fire protection and prevention unit. Again, the peculiarities of operations will generally have some effect on the type of fire prevention program necessary for a given location. This would not only include the physics of heat, but also a well-rounded fire safety program for employees. These procedures involve the knowledge of fire hazards, inclusion of brigade membership and a program designed to stimulate interest in fire prevention and fire protection practices.

A guard can be extremely valuable as an aid to the safety department. Furnished information regarding the basic hazards in the plant and the primary causes of accidents, he can automatically become a one-man safety committee and, through coordinated effort, contribute substantially to good safety and housekeeping methods.

At those locations where security regulations are a governing factor in adequate plant protection, we must be sure that all our guards can be readily cleared for required access to classified material if the necessity should arise. Since this is a closely controlled process, it is absolutely essential that our guards are completely trustworthy. The very nature of his work makes it necessary for him to visit all parts of our plants, laboratories and offices.

In the majority of companies where plant protection personnel are considered a part of the management family, they have not affiliated with labor unions. The nature of plant protection service is such that it should not be interrupted during periods of labor trouble. Sometimes it needs to be strengthened, not only in manpower, but in proper attitude. . . .

Most of us are well aware of what the resulting chaos would be if our municipal police and/or firemen were to completely shirk or desert their duties. The situation differs little insofar as the relationship between our plants and guards are concerned. Plant guards, properly schooled to always be fully conscious of their obligations, will not cause their employers to be apprehensive about their loyalty to their company or their country.

The continued activity of the communist element in this country certainly makes it imperative that we do all we can to familiarize our guards with the tactics used by those people who are bent on engaging in sabotage and subversive activities in industry. The infiltration of communists into certain labor union activities adds much emphasis to the importance of being able to ferret out the element which will do all in its power to enhance the cancerous growth of communism in this country—and then seek protection through the Fifth Amendment.

In summary, guards are no different than other management employees who, in order to perform at maximum efficiency, must remain constantly alert and be fully aware of all that is going on around them.

Through a well-developed plan of selection and training, we can develop public relations-minded guards who, like other conscientious employees, take pride in a job well done and properly reflect the spirit of the organization they represent.

THE GUARD FORCE, AS CONTRACTED SERVICE, By WILLIAM PAINTER, *Globe International Detective Agency*

I Theory governing "contract" guard service.

A. Generally same theory as in contracting for other services in industry; i. e. cafeteria or feeding service, maintenance services, accounting or audit services, and other services of a specialized nature, to get a better job done and frequently for less money.

B. Contract guard service is not new and has probably been in effect ever since guards or protection personnel have been used.

C. The primary reasons firms use a contract service today in lieu of company or individually employed guards are simplicity of operation and economy. No headaches regarding supervision (except from a policy standpoint) training and administration, and one low rate per hour.

D. A contract guard service is available from many firms on either a local or national basis and the quality of the service received varies from poor to

excellent, depending on the firm selected to perform the work and the rate charged. Again, just the same as purchasing any other service or item.

II How most contract guard services opreate.

A. Normally quoted on a rate per guard man hour. This usually includes: uniforms, firearms, personnel clearances, special police authorization, license and bonding fees and similar items that an individual guard needs to do his job.

B. The contractor assumes all problems for recruiting, training and equiping guards. All scheduling of work hours is borne by the contractor as is securing and furnishing replacement guards for vacations, sickness and other reasons for absence.

C. The client has control over policy and operations to the extent agreed upon in the contract.

D. Length of contracts vary but are usually for one year with a 30-day termination clause on either side, except for spot assignments.

III Advantages to a company or firm in contracting for guard service in lieu of operating a guard service itself.

A. Flexibility—the number of guard man hours used can be as variable as the requirement. Since the service is paid for by the hour, no certain number of bodies are required to be kept on the payroll.

B. Economical—pay only for the hours of work received. No fringe benefits to pay for.

C. Elimination of personnel problems—recruiting, scheduling, training, labor disputes and other personnel administration problems.

D. Greater efficiency—particularly in small guard force operations where protection specialists are not available, due to "know-how" of the contract agency, (if it is a good one.)

E. Obligation of the contractor to do a good job to perpetuate its own existence.

IV Disadvantages of a contract guard service.

No actual disadvantages; however, it sometimes presents a few *problems.*

A. Problem #1—Low calibre of personnel sometimes furnished by contractor, but this is usually due to a firm selecting the cheapest service available. You can get good service at an economical price.

B. Problem #2—If a firm has an existing guard force which is being replaced by a contract service, there is sometimes worry about releasing personnel or absorbing them elsewhere. (This is not always a problem as the firm and the contractor usually jointly try to absorb them.)

V Suggestions to those considering a contract guard service.

A. As when purchasing any service—investigate the reliability and reputation of the firm and the people who comprise it.

B. Thoroughly evaluate the proficiency of the guard service required and ascertain whether the contractor is able to furnish the personnel who can measure up to this requirement.

C. It may be advisable to talk with more than one prospective contractor, not necessarily on the basis of price, but on quality of the service rendered. Find out the criteria used by the contractor in hiring its personnel. How much supervision and training do they have, etc.

D. Above all, do not make the mistake of selecting the cheapest service available if you want good operations.

If you are required to get three bids, you are not necessarily obligated to select the lowest bidder.

"There is hardly anything in the world that some man cannot make a little worse and sell a little cheaper, and the people who consider only price are this man's lawful prey." (John Ruskin, 1819-1900).

WORKSHOP/SEMINAR V

MEETING THE PROBLEM OF COST, BUDGETS AND ECONOMY MEASURES IN MY SECURITY PROGRAM

An Address By BRIG. GEN. F. A. KREIDEL (RET.), *Raytheon Manufacturing Company*

The problem of meeting costs and instituting economy measures has been a continuous prime consideration of the Raytheon security department. In the first place, and this is basic, unless security costs are kept at the minimum required to provide adequate protection, we could contribute toward pricing our company out of business.

Industry, in general, is plagued with fast rising costs, not only in security activities, but in all other operations. My discussion will of course be confined to security costs which are a concern of the government as well as industry.

At Raytheon all Security Department costs are charged initially to the Department and later allocated to the operating divisions in accordance with the amount of security service used. Security operations are centrally controlled. Thus, charges against the Department are channelled through my office, and the Accounting Department provides a monthly report showing in detail actual expenditures by item, com-

pared with the Budget Estimate for the month, and the variance. They also report on accumulated expenditures by the item for the year with the variance in each case. Thus, for each of my operations, I know how we stand monthly and how accurate my forecast has been. Forecasts are made four times a year. In addition, I am required to submit a Medium Range (two-year) Forecast and a Long Range (five-year) Estimate. Under these conditions, "crystal balling" becomes a fine art. However, it is amazing how close you can come, provided you are furnished adequate premises.

The Raytheon Security Department is charged with all normal security functions except fire and safety with which departments we cooperate and coordinate. Thus, we are responsible for protecting all facilities against sabotage, subversion, pilferage and unauthorized entry. We establish security programs and objectives and assure their implementation.

An analysis of any security department's budget will clearly indicate where the director will have to devote his time to control costs. Payrolls, including overtime and labor surcharge, will run from 80 to 95 per cent of the entire budget. All other operating expenses will vary from 5 to 20 per cent. Since security is a service operation, depending to a large extent on men, not machines, these high payroll costs are anticipated and, if you solve your payroll control problem, you go a long way towards solving other expense problems since many of them fluctuate directly with the size of the force. I am thinking of uniforms, personal equipment, telephone, and travel expense. Certain operating expenses with which all departments are charged and over which we have no control such as general and administrative expense, occupancy and re-arrangement are left out of this discussion.

Of our total payroll, over 80 per cent is spent on guard force salaries which makes this the major consideration in controlling expenses. Wages, as well as other guard costs, have been constantly increasing, the problem is to keep these costs under control without losing efficiency and at the same time without sacrificing employee morale and good employee—management relationship. To put it mildly, this is quite a mission, particularly since the job cannot be done satisfactorily without obtaining increased efficiency all the way around.

The easiest and probably the poorest procedure by which to adjust guard costs is to lay off large numbers of men with the possible sacrificing of security. We are trying to avoid having to resort to that course by keeping continuously informed of future requirements so that adjustments can be made slowly and without a general upheaval. In the fourth quarter of last year, we froze the guard force after experiencing a one hundred per cent increase in 9 months even though our operations had expanded during the entire period. During the freeze, we took care of our expanding operations through resurveying the entire guard activities. This resulted in consolidation of posts where we believed duplication of coverage existed, the rescheduling of shifts, the elimination of Saturday and Sunday posts through locking seldom used entrances and in other ways which did not affect our over-all physical protection.

The freeze was raised after a period of 4 to 5 months. However, before we hire additional men, we take special precautions of not putting them on the payroll until they are actually needed. We are also attempting to utilize mechanical devices where conditions permit. We plan to transfer the men made available by use of this equipment to newly opened installations. We are continuing to take a new look, therefore, at electrical protection devices. We are resurveying our operations to ascertain where and to what extent they can be used. Finding contracting officers most receptive to any recommendation which would reduce cost without sacrificing security, we discuss the use of these devices in advance and use them in places authorized by the contracting officer concerned.

Part of the expense-control campaign is to indoctrinate personnel thoroughly with the idea that security is essential, but that it is also a service, and not a revenue-producing item,—but is rather an overhead expense; that all must cooperate to keep costs at a minimum in order to keep our company in a competitive position. We dispel the idea that, though some costs are charged back to the government in certain contracts, we do not have to worry about them. Through these means, we try to keep phone, travel, meals, supply and other costs at a minimum and, what is more important, we analyze actual costs monthly to assure that they are warranted. Keeping expenses down is team operation.

We have discovered another area which, in our opinion, has not been fully exploited and that is the elimination of unnecessary security measures. Of course, I am well aware of the fact that all security officers are taking all the action they can to prevent industry from being saddled with what we consider to be unnecessary and extravagant security procedures. That is a continuing obligation and one of our prime responsibilities.

I believe the ASIS* and the security committees of the industrial associations such as the Aircraft Industry Association, the Electronics Industry Association and the National Security Industry Association have done an outstanding job of working with the department of defense representatives toward this end. Frequent consultations between DOD** representatives and security representatives of industry will result in a realistic, logical application of the government's security program. We are all vitally interested in the same results—maximum security at minimum cost to make our defense dollar most productive. When we encounter a serious problem, we discuss it with our cognizant security office and the contracting officer or his representative and come up with a sound solution beneficial to the government as well as the company.

*American Society for Industrial Security
**Department of Defense

We feel this is a most important responsibility of security directors, for frequently such actions result in our seeking amendments or changes in the manual regarding those measures which we consider to be unnecessary and expensive.

We are finding that our security representatives can materially assist in reducing their problems by establishing far closer working relations with each plant's negotiators and contracting office representatives. The objective is to reduce the number of classified items on the security requirements check list DD Forms 254. The DD 254 provides for its reexamination every 6 months during the life of the contract for the purpose of reducing classification of items or declassifying items entirely. We also know that in a great number of instances contracting officers have delegated to their representatives in industry's plants authority to approve declassifying requests. In many instances, this can be readily obtained if the contractors, negotiators, engineers, or security representative submit a request with ample justification. I have found instances where we have not utilized this opportunity to the fullest extent possible. Reduction in the number of classified items tends to reduce security costs.

I wish to pay tribute to Buaer's* New Classification Guide and its efforts to reduce the number of items classified. We have experienced unusually fine results in our Buaer and Army Ordinance Contracts and expect to do equally as well with our other contracting officers.

*Bureau of Aeronautics

In our contracts, we have noticed that the classification "Confidential Modified Handling Authorized" is very seldom used. Hardly any documents are so marked and practically no equipment. I feel certain that in most instances contracting office representatives who will not agree to declassifying secret and confidential items will reduce some of them to CMHA. Of course, the accomplishment of this objective reduces the storage requirements and the expense of combination lock file cabinets and accounting measures.

It is understood that the Department of Defense proposes eliminating accountability for confidential material in the next revision of the manual. I was greatly surprised to find some directors of security opposed to this revision claiming they had systems capable of accounting for this material and wished to keep them operating. There is definitely great cost involved, and I am sure security men can find use for personnel freed from this administrative work and place them where they can assure tighter security for secret and top secret information. The government's intention to expand research and development activities would indicate there will be increases in the number of secret and top secret contracts, documents and material.

In conclusion, I wish to say that budgeting and control of expenses is a top priority requirement of all Raytheon department heads. In security, my job is first to assure that our company fully meets the DOD security requirements and secondly, that we accomplish this objective at minimum cost to the company and the government.

An Address By LAWRENCE P. BUCHMAN, *The Martin Company*

We are all aware, I believe, of the intermittent controversies which have existed between the government and industry whenever the Industrial Security Manual has been revised by the Department of Defense. The critical attitudes which have developed at these times have often served a useful purpose. In some instances they have resulted in major modifications of the original revision, and thus have helped to shape the program as it has evolved in the last five years. In other instances industry, after experience with the change, has found the new procedures to be not nearly as burdensome as originally supposed. The important thing about this "give-and-take" has been the development of a partnership program which, after all, is the only effective program.

While this evolutionary process has been extremely fruitful, there are still areas in the program which warrant further study. One such problem area lies in the present method of financing security costs in industry. While the importance of the security cost problem may have been generally overlooked, it is one of the major factors which has prevented the Department of Defense from realizing its full policy objectives in the field of industrial security. In addition expenditures for security by the Department of Defense is well over one billion dollars per year at present. In the light of forty billion dollar annual defense budgets, it is extremely important to use the security dollar with maximum effectiveness. With this in mind, let's examine some of the factors which shape the partnership attitudes on questions of security costs.

As background, it should be realized that most firms treat security expense as an overhead item. By this I mean that a $100 item for security labor is not put on an invoice and sent to a military contracting officer for payment. Usually this would not work because the labor item would be applicable to more than one prime contract, and it would be virtually impossible to prorate the charge on an equitable basis. To avoid this accounting difficulty, security expense may be lumped with such other overhead items such as maintenance and personnel administration. Then, based on experience factors, the contractor charges total overhead to each prime contract on the basis of a fixed percentage. Usually the percentage is applied to the cost of direct labor. The firm's income for the security budget, therefore, consists of a certain percentage of whatever direct labor happens to be assigned to the contract in question. If direct labor

drops, security income on that contract will also drop. If direct labor increases, security income increases. It is important to note that these fluctuations in security income are not in any way dependent upon what the contractor must spend for security. This is established by an entirely separate contract document, the DD441. Past experience dictates that changes in the DD441 have resulted in a gradual but continuous increase in contractors' expenditures for security and that this process will continue.

The practice of handling security expense as an overhead item has one very important effect. Since the contractor's security income is based on an overhead percentage computed at the time of the original bid quotation, security income tends to be exceeded by security costs as the contract progresses. This can be caused by revisions of the DD441, or merely by new interpretations of the regulations by the cognizant agency. In a sense, therefore, security expense is unique, and is governed by factors which do not affect any other type of overhead expense. Whenever expense tends to exceed income, the cognizant agency will meet increasing resistance from the contractor as new methods to improve the firm's security program are suggested.

The cognizant agency has been told that the government is underwriting the cost of the security program. They do not understand how security costs can exceed income, and therefore feel that the cost argument may be an effort to evade responsibility under the security agreement. These misunderstandings create unreasonable friction at the local level and do much to harm the program.

At this point, to answer the cost argument, the cognizant agency may well say, "Mr. Contractor, you claim your costs exceed income. Here in Section VI of the agreement it says that you can recover your increased security costs under the substantive contracts. Why don't you seek relief from your contracting officers?"

The answer to this question is rather complicated. Consider the case of a major defense contractor with perhaps 100 contracts, ranging from unclassified to Top Secret, spread among the Army, Navy and Air Force. Assume further that the increased cost item amounts to $75,000 per year and results from a revision of the DD441 which affects all classified contracts administered by seventy-five different contracting officers. The problem of attempting to furnish an accounting back-up to justify a method of prorating the seventy-five shares would be almost insurmountable. The contractor would have to be prepared to furnish information which in many cases is unobtainable. The Contracting Officer may ask, for example:

1. Who is coordinating this over-all claim on behalf of the government? (No provision exists in the regulations for such coordination).
2. Is there any precedent for an arrangement of this type? Is it permitted under the regulations?
3. Will the other contracting officers refuse approval? Shouldn't my action be coordinated with theirs? How should this be accomplished?
4. Does the contractor keep the type of accounting records which permit a contract-by-contract breakdown of the total charge? (Probably not. What share of an eight-hour day on patrol by a guard can be assigned to the contracts, and what part to the contractor's own interest?)
5. If such records are not available, how was my pro rata share established?
6. Shouldn't the charge accessed against my confidential contract be lower than for a contract involving classified hardware and area controls? (Yes, but on what basis should the division be made?)

The Security Director who contemplates creating this type of problem must measure it in the light of his firm's customer relationship and probably customer antagonism. Remember that the separate claims may be as small as $1,000. He must bear in mind that in his own organization his performance is measured by the degree of common sense he exercises. In the eyes of management, at this point, the Director's only problem is one of living within his security budget. Management would much rather "stimulate" the Director's budgetary consciousness, than risk antagonizing seventy-five customer representatives for a relatively insignificant claim. And yet the aggregate amount is substantial. The conflict between these two alternatives, unfortunately, may encourage some contractors to come into compliance by cutting the cost of security services in other areas where they will be least noticed by the cognizant agency. If additional violations result, and an attempt is made to reinstate the cancelled service, the cognizant agency is again on the cost merry-go-round. Nothing has been solved.

The mechanical difficulty of negotiating reimbursement for increased security expenses under present Department of Defense procedures is not the only factor which shapes industry attitudes. It is not even the most important factor. Once the overhead concept has been accepted as the only method of financing security expense, then also accepted is a system which tends to place firms in the same industry in competition to cut security expense. Since Security forms a part of the overhead quotation on all bids, other things being equal, awards will go to the firm with the lowest overhead rate. This is almost tantamount to stating that firms with the *cheapest* security operation have the best chance of getting new Department of Defense business. This paradox is certainly not the intention of the Department of Defense. Yet industry, after listening to all the fine speeches, reacts most strongly to actual procurement practices. In this respect some contractors look upon a self-imposed increase in overhead rates as a form of competitive suicide. Therefore, even if more security funds were available for the asking, the resulting increase in overhead rates might dictate some other, more prudent, solution to the security budget problem. All this, of course, is extremely difficult to explain to most cognizant agencies.

To summarize, we can emphasize the following facts.

1. In industry, security costs tend to exceed security income as the program evolves.
2. Mechanics have been established to recover such excess expenditures, but the problems of customer relationships, and accounting justification, make the approved procedure unrealistic.
3. Most firms treat security expense as an overhead item. This practice is mandatory because security obligations are set out in one contract document, and reinbursement is provided in a set of totally unrelated contract documents.
4. Treating security expense as overhead places security on a competitive basis, and places a premium on the "cheap" security operation.
5. Even assuming that present procedures for recovering excess costs are adequate, (which does not seem to be the case), competitive considerations would preclude many contractors from using the procedure to better their security operation, because the increase in overhead rates would make them non-competitive.

Perhaps the answer to these problems is to divorce security compensation from all substantive contracts. Security costs would then be negotiated separately as a part of the security agreement, and would be paid by, and through, the cognizant agency in proportion to the service required by that agency. A host of contracting officers would be relieved of all secondary security obligations, and authority would be centralized in a staff of trained security specialists. This would insure adequate government supervision of all security expenditures. It would correct the published finding (by the Wright Commission on Government Security) that, "Such cost figures were unobtainable because neither the Department of Defense nor the Armed Services maintain them. Figures made available to the Commission . . . . gave only a partial cost picture at best, and reasons advanced for such deficiency were both illogical and unpersuasive."

Other achievable results from eliminating the competitive aspects of overhead financing might be:

(1) An improvement in management attitudes toward the program.
(2) Less resistance to unilateral government changes in the security regulations.
(3) Shift of cost supervision from firms affected by the regulations to the agencies responsible for writing the regulations.
(4) Establishment of a central authority from whom the contractor can seek relief on security fiscal matters.
(5) Elimination of complaints on the legitimacy of the security agreement as a true bilateral contract.
(6) The placing of the Security Director in a position to achieve the government's security objectives without cost interference.

Such potential benefits would indicate that the present method of financing security costs should be scheduled for joint study by industry and the Department of Defense.

An Address By HARVEY BURSTEIN, *The Massachusetts Institute of Technology*

Our discussion this morning is concerned with the problem of costs, budgets, and economy measures in security programming. I feel that initially we cannot but take cognizance of the fact that a security program is an expensive item in any enterprise. This question of expense is just as applicable to the academic institution as it is to the manufacturing plant or retail store.

There are differences, however, between security programs concerned with the protection of classified material, and those concerned with problems of plant protection generally. The Massachusetts Institute of Technology is confronted with problems in both areas. Much work has been and is being done at M. I. T. under contracts with the Federal Government. On the other hand, we also have a sizable community that is not concerned with classified work for whom security services must be made available. Another factor in the security picture at M. I. T., or any other academic institution, is the fact that a university will be confronted with problems that are somewhat unique, and which have no equivalent in the industrial establishment.

Two vital factors are found in connection with problems of costs and economy measures where security for classified programs is concerned. The first is a realization of the fact that much of the program generally is pre-determined by the security requirements of the federal agency, or agencies, involved. The other factor is related to the contract itself inasmuch as all or part of the security program may be considered by the contractor as a reimbursable item in one form or another.

These factors are not present in the security program relating to plant protection generally. In the latter instance, the expenses must come from the organization's operating budget and must be viewed as an overhead item.

To discuss briefly some of our problems at the Massachusetts Institute of Technology, I should like to reiterate that our position as an educational institution, rather than as an industrial establishment, has an effect upon our total program regardless of whether the security involves classified work or plant protection generally.

For many years M. I. T. has been engaged in research for various agencies of the Federal Government. The program, however, has not remained static. Differences in the size of the projects, their physical location, the level of the classified work involved, and their total programming all have had a bearing upon our problems of costs and budgets, and have controlled, to some extent, the economy measures which could be instituted.

For example, as an educational institution we have made every effort to house our classified laboratories on the fringe of the campus rather than in its midst. The physical separation of some of our laboratories, and off-base sites, from the campus itself sometimes is rather considerable. On the other hand, there are some relatively small undertakings being handled by a limited number of people, in an equally limited area, which do result in some classified work being performed in areas normally considered as academic. Another factor, aside from location, is the frequency with which research programs require an around-the-clock effort.

The physical location of our larger laboratories, and the 24-hour operation of many of them, have made it quite obvious that reliance upon any form of protection other than guards is impractical. In other areas, even though alarms may be used, we must recognize that as mechanical devices they are subject to failure, or can be rendered inoperative, so that it would be imprudent not to continue some form of guard coverage, albeit in a limited form.

Guards, security education programs, security-type equipment, and the storage of classified material, are the principal areas of expense in the classified security program. Let us briefly consider them as such.

I believe that most security administrators will concede that the expenditure of salaries for guards constitutes the largest single expense in the security program. They also will agree that qualified, high caliber personnel cannot be obtained unless they are offered a better than living wage. To economize on salaries is unwise, and can prove to be more expensive than the salaries themselves in the long run. In addition, where guards are concerned, there must be an allowance for the fact that an individual can do only so much work in a given period of time. We also must recognize that normal human problems occasionally prevent a man from reporting for duty. It is not uncommon for situations of this sort to create problems leading to overtime, and the very fact that these situations cannot be anticipated with any degree of regularity makes any accurate allowance for overtime in budget planning difficult. All of this means that economies in connection with guard service must be obtained in other ways.

The guards assigned to our classified areas are armed and deputized. To furnish a guard with a weapon and authority without training him is to risk potential embarrassment, or even trouble, for the employer. For years the M. I. T. guards have undergone periodic firearms training and during early 1957 a course of formalized classroom training was initiated. In order to accomplish training, while maintaining security, it became necessary to handle a large part of the instruction on an overtime basis. The results have more than justified the expense; however, the expense involved does preclude our giving such formalized training to each individual addition to the guard force. Consequently, in order to do something about meeting the problem of training without incurring additional expense we are issuing a written handbook to each guard outlining in detail their duties, responsibilities, and limitations. Firearms training, however, continues for all personnel.

All Institute personnel newly employed in classified areas attend a security orientation lecture presented by the M. I. T. Security Office. Aside from this general discussion, however, we find that we can obtain more effective results for less money by permitting the various laboratories to handle their own security education programs. These several programs are the responsibility of the laboratory administative officers to whom the security program has been delegated. All of these programs are conducted in accordance with the security policies recommended by the Institute Security Officer and approved by the M. I. T. administration.

The purchase of security-type equipment must be considered when thinking in terms of costs and budgets. M. I. T. does not skimp on equipment of this sort; neither does it go to the other extreme by purchasing items for which we have no immediate use, or which might best be described as "fad" items. The equipment purchased always measures up to prescribed standards and there is no reluctance to spend a little more on money for a lot more in value. By the same token, coordinating all purchases through a Property Officer frequently enables us to salvage excellent equipment that has been used in a discontinued classified project for use in a new or expanding program.

The storage of classified documents is an additional problem in virtually every classified area. Guard coverage, security equipment, and the time and effort expended in protecting classified documents can become very expensive. It is even more of an expense when the documents involved no longer are considered as active files. In an effort to combat this expenditure of funds and space we constantly seek ways of returning inactive or excessive copies to the originator of the document, or else we make every effort to destroy that for which there is no need, maintaining detailed certificates of destruction.

It would be safe to summarize our position insofar as classified security is concerned by saying that the Massachusetts Institute of Technology constantly strives to render maximum protection at a minimum cost with due consideration for all of the numerous factors involved.

The problem of adequately protecting that part of the Massachusetts Institute of Technology not involved in classified research is more complex. Funds for this phase of the program must be provided from within the Institute. As a non-profit making educational institution, funds are limited. Monies received from grants and endowments usually are restricted to specific use for academic purposes. In addition, the nature of the work itself presents problems not found in connection with classified security.

In order to achieve a better understanding of the problems of costs, budgets, or economies as related to this area of security, it is necessary to know something about the total picture at M. I. T.

The Massachusetts Institute of Technology constitutes a community of approximately 10,000 people working or studying within the confines of a 100-acre campus in the City of Cambridge. This campus is in no way enclosed. The Institute is bounded on three sides by the City of Cambridge, and on the fourth by the Charles River. Directly across the river is the City of Boston. Consequently, the campus must be considered as more than a city within a city; it is a city whose total property value, both real and personal, exceeds the property value of the average community of comparable size. In addition, the total population of the communities comprising the metropolitan Boston area far exceeds a million and half persons. As a result of our location, we find that our plant protection problems cannot be compared to those of the educational institution situated in the so-called "college town." Our plant protection problems are more like those found in the average metropolitan police department and, on a smaller scale, our budgetary problems also are similar.

As in the case of guards, salaries are our principal expense and attempted savings on this item prove to be false economy. However, in an effort to meet this problem, M. I. T. has reacted in two ways. Not only is our wage scale comparable to that in private industry for similar work but also we have recruited personnel primarily from among retired servicemen and police officers. The combination of pension and salary provides us with men who find their income more than adequate, thereby keeping down that expense normally found where a quick turnover in personnel results.

I have mentioned the difficulty in allowing for overtime insofar as our guard force budget is concerned. The inherent nature of police work on a campus or in a city makes it even more difficult to anticipate emergencies or other items which involve overtime and for which budgeting provisions must be made. The administative organization at M. I. T., however, is such that on numerous occasions a transfer of funds can be arranged from a department to the Security Office in cases where we have rendered special services in the form of details.

Unlike the short cuts available in training guard force personnel, campus police must be given formalized classroom training. It is true that both groups are armed and deputized; however, the very nature of the campus police officer's job makes the exercise of authority a more prominent factor in his daily activities and requires that he be fully cognizant of his responsibilities and limitations. Training personnel is an expensive undertaking, but again we have found that the selection of retired servicemen and police officers has enabled us to give a maximum course of instruction in a minimum period of time. It is only in this way that we can hope to meet the problem of training costs.

The members of this unit are uniformed. This presents an expense with which we are not confronted insofar as our guard force is concerned. Various points must be taken into consideration in uniforming personnel. If the unit is to represent properly its employer, and if the men take that pride in their appearance which also reflects favorably upon the employer, practically dictates that a single uniform issue is insufficient. Allowances also must be made for the fact that replacements will have to be made for damaged or lost property. We have discovered that by purchasing a better grade of uniform initially, we are not confronted with the need for rapid replacement. This, coupled with an adequate clothing issue, has proven to be an economical approach to our uniforming problems. We have minimized losses and the expense of replacement by holding personnel individually accountable for all property furnished. For example, if a man loses or damages an item of property or clothing in line of duty, M. I. T. stands the cost of replacement. If, on the other hand, it is due to the officer's carelessness or misuse of property, he personally must replace the item lost or damaged.

The area of plant protection generally presents other factors which involve expense to management. A police force, be it a campus police force or a regular department, is virtually helpless without some communication and transportation. In order to render maximum service to M. I. T., our uniformed group uses a cruiser equipped as an emergency ambulance and having a two-way radio. The use of this vehicle on a twenty-four hour basis means considerable expense insofar as operating costs are concerned. Its constant use also means that repairs will have to be made from time to time. These items, of course, are in addition to the normal allowances for registration and insurance. There is no practical way to effect economies in the operation of such a vehicle without reducing the extent of service rendered by the organization. We were able to effect a saving in connection with the installation of our two-way radio. The Cambridge Police Department graciously agreed to permit us to transmit and receive on their frequency and to use their dispatcher. Not only has this resulted in a saving to our program, but also it has proven mutually beneficial to the organizations involved.

There is an aspect of security programming, whether it be in the area of general plant protection or the safeguarding of classified information, which sets security apart from other phases of operation in either the academic institution or industry in general. Regardless of the dollars and cents limitations which may be placed upon the program, and regardless of the effect of any economies no matter how justified, personnel charged with carrying out the security responsibility must see to it that the work is done effectively. To eliminate a security program as an economy measure may well prove to be more expensive to the organization, over a period of time, than would a continuation of the program itself.

At the Massachusetts Institute of Technology we try to meet the problem of costs and economy measures by following certain basic precepts which are inherent in good management generally. We have applied these principles, insofar as is practicable, to both phases

of our security program. They can be summarized as follows:

A. We never make any requests involving an expenditure of funds without having first satisfied ourselves that this expenditure is absolutely necessary in order to enable us to discharge our responsibilities.

B. Once we have determined that an expenditure is necessary, insofar as is practicable, we attempt to get bids on the items to be acquired.

C. Before making any purchase we satisfy ourselves that the items to be purchased not only will satisfy our immediate needs, but also are of sufficient quality to permit us to obtain maximum usage over a period of years.

D. We try to weigh the expenditures involved, on the one hand, against the projected expense to the Institute if we do not follow through with this phase of the program.

E. Where salaries and fringe benefits are concerned, we try to make jobs sufficiently attractive so as to minimize the expense involved in a rapid turnover of personnel. We also consider that in many instances we can render better protection to M. I. T., for less money, by working some of our personnel on overtime as against acquiring additional manpower.

F. Administratively, we attempt to use standard form letters and all of the other related short cuts possible so as to render maximum service at minimum cost.

Our experience at M. I. T. has been a happy one. By following the principles outlined above, the M. I. T. Security Force has rendered maximum service at minimum expense; by the same token, it has been observed that none of our requests for additional funds have been denied us so long as we could justify clearly the reasons for requesting the right to make such expenditures.

The importance of the security program and the ultimate savings which it can make available to management do not justify any security officer spending company funds with a complete disregard for the return. However, a properly organized and integrated security program should be able to justify its existence by virtue of the services rendered. No matter how important the security program may be, good business practices require that the total cost of the program be a legitimate and proportionate part of management's over-all operating budget. To do otherwise is imprudent, impractical, and economically unsound.

An Address By R. J. LAVOIE, *International Telephone and Telegraph Company*

As is pertinent to the U. S. Group operations I find both questions relatively easy to answer. Each of our locations in the United States employs trained and experienced security specialists on a full time basis. While the operations in these locations are greatly diversified, the coordination and similarity of security programs permits a flexible well controllable budget. Through a series of recurring reports submitted to my office, frequent trips performed by myself and frequent, informal meetings of security personnel, we have been able to develop security programs utilizing the best known modern methods at a cost which is under constant scrutiny and receives full support of top management.

Those of you who are responsible for multi-facility operations within the United States with Department of Defense classified contracts may find that varying interpretations of the Industrial Security Manual by differing cognizant security offices is an area in which considerable savings can be effected. ITT is covered in its various locations by representatives of the Army, Navy and Air Force for the Department of Defense as well as the Atomic Energy Commission.

Within the three Department of Defense agencies I find myself confronted with diametrically opposed points of view in the various interpretations or applications of the provisions of the Industrial Security Manual. These interpretations for the most part are well meant by the government representatives; however, some of the recommendations made by some overzealous inspectors often result in considerable expenditure of funds. There are many examples of these that I could quote to you but I am sure you have been exposed to these in your own operations.

Whenever possible my office attempts to resolve these matters amicably at local level indicating that their brother services who operate under the same manual have not required these additional or expanded security measures. If I am unable to resolve these matters to the mutual satisfaction of industry and the cognizant security agency at local level, I request the assistance of Mr. Applegate's office in the Department of Defense. While the Department of Defense is not desirous of supervening over any individual service they can and will act in an advisory capacity to them indicating that it was not the intent of the manual to impose these additional security requirements.

In the many countries outside of the United States where ITT has installations we have an equal need for security systems. . . . Recommendations made by my office for the establishment of procedures which are utilized with great success in the United States and which generate efficiency and reduce cost, are in many instances contrary to national laws, legal statutes, national defense regulations, union problems, retirement programs, labor laws, political interest, and so forth.

Some of our foreign companies for example are involved in North Atlantic Treaty Organization security regulations, others are involved in off-shore procurement contracts of a classified nature and last but not least most of them are engaged in one form

or another in numerous contracts of a classified nature under *national* classification which even the President of our company has no need to know—not to mention myself as the corporate Security Officer.

While these matters do not necessarily prohibit the operation of effective and financially sound security programs, they cause the presentation of corporation budgets on my part to be greatly inconclusive.

At the present time, I am reviewing on an individual basis the various budgets pertinent to security submitted by each operating company. It is my hope that I may finally arrive at a yardstick or pattern within foreign operations whereby I may judge the dollar-and-cent value of each security program. While I am usually in a good position to tell my boss what our programs are costing us, I am often unable to inform him whether or not it could be done at a greater saving to the company.

You may appreciate this problem a little better if I illustrate the budget review of one of our smaller manufacturing companies overseas. This budget for a fiscal year revealed that by virtue of its total output in dollar value, number of employees, square feet of manufacturing area and other pertinent details, that the number of guards employed approximated 92% above a similar operations in the United States. Thinking that this might be a fine example to use, I posed a series of pertinent questions to the General Manager of Operations. In brief my questions dealt with fencing, electronic controls, closed and restricted areas, number of guard personnel, rates of pay, authorized vacation time, and overtime clauses. Much to my surprise I was informed (with local indignation) that the security force was felt to be inadequate based on the following:

a. Two of the national defense classified contracts would not permit the utilization of electronically controlled devices.

b. While fencing had been installed some years ago, the guards utilized as a supplement thereto were long-term employees who could not be released due to a pension plan and were kept on the payroll until their pensions were consummated. The rates of pay for guard personnel were established by local labor laws and were on a par with guard personnel utilized in commercial banking institutions. Overtime clauses and vacations had been written into the last negotiated contract and, in order to reduce the overtime, additional guards would have to be placed on the payroll. Needless to say, after much correspondence between my office and Europe I felt that the best I could do under the circumstances was to forget about the whole thing.

In conclusion I wish to state that we have in the past, and continue to receive the full support of ITT management for all reasonable expenses incurred in the security field. In the presentation of these budgets we define "reasonable" as those items which can be justified as contributing to *successful* and *profitable* operations.

Whenever any item of expenditure falls in the questionable field—it is roasted and fried until we can get to the core of it and ascertain whether there is a real need for it—or whether it is just another luxury we can ill afford.

Finally, the opportunity to get together at this conference, as well as other informal meetings of security specialists, the exchange of ideas, profiting by someone else's failures or success, is the further key to the constant development of better security to our nation and to our respective companies.

An Address By C. L. BRADSHAW, *The Aluminum Company of America*

For some time prior to the beginning of the present business recession, we had become well aware of the fact that plant protection in our various facilities was not as effective or as efficient as it could be. This was evidenced by the fact that certain jobs not specifically a function of plant protection had been shifted over to our plant protection departments. At a number of plants there was poor utilization of time by men on their jobs and they were not alert and well trained in doing a thorough job. This situation, I am sure, is not unique in our company.

As a part of our over-all security responsibility we had initiated a company-wide program to correct this situation which included the following major aspects:

Selection of better qualified personnel, including (1) elimination of the practice of unloading people onto the plant protection staff for whom jobs could not be found elsewhere in the plant, (2) more thorough training in job responsibility and duties, (3) periodic evaluation and appraisal of employee performance; and (4) administrative improvements—better scheduling and controls, assignment of more responsibility and better use of time, better records of work accomplished, and the use of mechanical and electrical aids.

Up to the time of the first serious reduction in our plant protection forces, we had made considerable progress with this program. Through a plant protection committee made up of our better chiefs, we had developed a handbook for use company-wide and we had taken this program to most of our plants where it had been presented to interested management personnel. Probably the main thing we have accomplished so far is an awareness of the need for improvement and the possibility of getting more for our plant protection dollar. Many of our plants welcomed the program and immediately set about putting it to use.

We were, therefore, somewhat prepared for the rather extensive reduction in our plant protection forces, most of which occurred during the early part of this year, and while this reduction did seem rather serious it was no more so than the general reduction of personnel throughout the plants.

A variety of things have been done to adjust to the

curtailment of plant protection budget. These might be classed in two general groups, namely, elimination of certain duties and responsibilities and more effective utilization of the remaining guard force through the program referred to above. In the first category we found it necessary to close certain plant entrances and eliminate guard stations either entirely or in some instances only between shifts. In some cases call signals were installed at closed gates so that an employee or truck requiring admission to the gate could call for someone to open the gate if necessary. In one case the control of a gate has been assigned to a first aid attendant where such attendant was readily accessible.

Numerous responsibilities have been turned back to other departments. For example, operating and maintenance departments are assuming more responsibilty for fire fighting and other fire-protection duties. Production supervisors are taking back some of their fundamental responsibilities which to some extent had slipped over the line into plant protection. Bulletins are being posted by the departments issuing them. Time-keeping departments are responsible for delivery and picking up time cards; driving of station wagons and variety of messenger work is being turned back to the department more directly requiring these services. Reduction of production and maintenance work on the (B) and (C) shifts plus better control in requisitioning materials have reduced the need for guards to serve as emergency storekeepers.

Fire patrols have been appreciably reduced with the approval of the Insurance Company. Patrol routes have been rearranged and in some cases stepped up with the use of motorized equipment. Use of shortwave equipment has also facilitated the communications job. The plant protection supervisors occasionally have found it necessary to pinch-hit for guards, and other personnel around the plant have been assigned plant protection duties during the periods of shortage due to vacations or illness.

In the second phase that I mentioned previously, we are trying to make more efficient utilization of our present guard force. So far we have not had an opportunity to do anything in the way of selecting better personnel, but through training we are slowly developing a more reliable and effective guard force. Better planning and scheduling of time will effect more efficient utilization of the guard's time and through better administration and training we expect to make far more effective use of plant protection personnel ability.

Furthermore, we expect to improve those areas of security and plant protection not directly under the supervision of the plant protection personnel by making production, maintenance and office supervisors more cognizant of their responsibilities for the protection of employees, equipment, jobs and security information and by better communications and closer liaison between supervisory and plant protection personnel.

Our ultimate goal is to do the same job with fewer men than we were doing before the recession and to do it more effectively. Until we get geared up to offset the current loss of personnel by doing a more effective job, we will be taking some additional risks, but in the long run we expect to be able to do a much better job and at a lower cost. In other words, we intend, as we have from the start of our company-wide program, to "get more value from our plant protection dollar."

WORKSHOP/SEMINAR VII

Part One — FIRE

THE DETECTION AND CONTROL OF FIRE HAZARDS, By JOHN L. BRYAN,

Professor, University of Maryland

I would like to emphasize the last two words in the title of this presentation for a moment in an attempt to clarify our thinking and orientation to this important subject. We are examining fire hazards and not the detection and control of fire which is an entirely different proposition and requires different concepts and premises. In fact, when we have a fire occurrence this means we have had one or more fire hazards in existence for some time, and this fire is the result of these hazards. We may think of this concept as a continuum in time with human activity at one end of the continuum and a fire occurrence at the other end. Thus, it is our concern or problem to break the continuum with the removal of the fire hazard from the chain of events. Of course, before the fire hazard may be controlled, it must be recognized or detected. The duty of industrial fire and safety personnel in this respect is very similar to the sentry on outpost duty in which he must distinguish his friends from his foes. The problem is complicated since fire and fire-orientated processes are the basis of our industrial achievement and yet we must detect the situation where fire may destroy our industrial facilities and organization.

It is important at this point for us to attempt to formulate a definition of a fire hazard.

For the purposes of this paper I would like to offer the following definition for fire hazard: "A condition, factor, or combination of such conditions and factors into a situation that is conducive to the ignition and propagation of a fire. Also conditions or factors that may be detrimental to the control and extinguishment of a fire occurrence."

Thus, it may be seen that for any environmental condition we may consider fire hazards fall into

two broad basic classes. The first type of hazard affects the probability of a fire occurrence, and the severity and degree of fire propagation. The second type of hazard contains the factors that affect only the severity and degree of fire spread, since it includes the factors that affect our protection and control equipment and operations.

I would like for the sake of clarification to give an illustration of hazards that might fall into each classification. In the fire class of hazard would be the factors of fire cause such as poor housekeeping, careless smoking, improper wiring and fusing, etc. In the second class of hazard we would consider the factors of closed automatic sprinkler valves, blocked fire hydrants, and untrained fire brigades.

Now you will undoubtedly notice that I have listed intangible conditions and factors in these classes as well as the usual tangible conditions we generally think of as fire hazards. This is because upon examination of the fire records and from experience it has been observed that the intangible factors of interest, attitude, and motivation on the part of the employees, management, and even our protective personnel are responsible for the creation and continuation of the majority of the fire hazards in our industrial communities today. Therefore, it appears important that we focus our attention on the human and psychological factors of fire hazards, as well as the physical, environmental factors of fire hazards.

The detection of fire hazards is usually dependent in most instances on the judgment and observation of trained protective personnel. In some specific installations we have automatic devices such as automatic combustible gas indicators on ovens and other installations which warn of the presence of conditions conducive to the fire occurrence. Thermostatic, and excessive heat controls are also found on specific installations. However, the automatic controls and devices for the detection of fire hazards are limited by construction and application to a very small area of any industrial environment. Thus, it can be seen that the bulk of our fire hazard detection effort depends on the efficient, and intelligent use of trained human observers.

The problems in the detection of fire hazards center into two general areas. First, does the observer cover the entire environment of the industrial plant at all times during and after operations? Fire hazards cannot be detected outside the range of the protective personnel's senses. In this regard the observer must be trained to use effectively all his senses. Secondly, does the observer recognize the fire hazard when he detects it? This recognition involves the complexity of the entire problem of fire hazards in our constantly changing industrial environment. It involves the problem of evaluation. This must include the materials being used, the environment in which they are used and the way in which they are used, or the process or operation being employed.

The detection of fire hazards for any industrial or nonindustrial situation may be generalized into the following important factors:

SELECTION—Personnel to be employed for the detection of fire hazards must be carefully selected for intelligence, adequate background of education and experience, physical condition, and a sincere interest and belief in fire protection.

EDUCATION—Personnel must be educated and trained in the specific problems and processes of your operation, in addition to the basic principles of fire protection. Personnel must be trained to evaluate and analyze your situations. Training should be realistic and should take into consideration both physical and human factors.

ORGANIZATION—The over-all needs of the envirment must be recognized and considered for the detection of fire hazards, as well as the organization's frequency of surveys, new processes, construction, and changes in company policy and practices.

AUTOMATIC DEVICES—The installation of automatic and auxiliary devices and instruments for the detection of hazardous conditions should be initiated whenever possible. Proper schedules for the maintenance and testing of such devices are necessary.

At the present time the detection of fire hazards is largely dependent on the intelligent utilization of trained fire-protection specialists. However, in the future more automatic devices will become available for the detection of fire hazards in industry. The development and utilization of such devices requires imagination and foresight on the part of everyone concerned with industrial security in the United States today.

We have spent the preceding time concerning ourselves with the detection of fire hazards, and it now appears important that we consider in a general way the control of fire hazards. It is obvious that we must not only detect fire hazards; we must also control them to prevent the ultimate occurence of a fire. The control of fire hazards by suggestion implies the removal, elimination, or isolation of the dangerous conditions or factors.

The principle of control for fire hazards generally applied in most situations is based on the separation of sources of ignition from sources of fuel. However, in some specific situations it is possible to control the source of oxygen necessary for combustion by inerting the atmosphere with the use of an inert gas. It is helpful in devising methods of controlling fire hazards to classify the fire hazards in your situation as ignition or fuel hazards. An example of this principle in practice might be in an area where flammable solvents were used to eliminate sources of ignition with the proper enclosed motors and explosion proof electrical devices, grounding devices for static electricity, controlled ventilation, and control of open flames from sources, such as smoking.

A secondary principle to be utilized in the control of fire hazards is found in all fire-protection planning. This is the principle of subdividing dangerous or hazardous materials in storage or in an industrial

process. This principle is based on the premise of limiting the propagation of the fire if the primary control for the prevention of ignition fails in the situation. The isolation of hazardous processes which are necessary to the operation of the industry is based on this premise of division.

The control of fire hazards imposes certain definite responsibilities upon the protective organization. The protective personnel must be able to defend their statement and recognition of a condition as a "fire hazard" and they must then be prepared to offer a safe and satisfactory evaluation of the situation for corrective action which will not conflict with the basic purpose of the industry. In other terms, because you state that a condition is a fire hazard do not expect this to be taken on face value by the production employees. You must be able to explain the facts and reasons for your conclusion and your labeling of the situation as being a fire hazard. Then once the fact of the existence of the fire hazard is established you must be able to offer a sensible, concrete plan of action for the control of the fire hazard. By a sensible plan of action we mean a plan that is not impractical to the operation of the industry.

Now, it is apparent to all of you that the control of fire hazards is not a simple task. This operation is always very complex. Factors of cost, economics of operation, employee relations, and management policy all complicate the situation. The protective personnel must formulate a plan for the control of fire hazards considering all of these important factors, and at the same time never forgetting their principles of fire prevention and safety.

The control of fire hazards suffers from two general misconceptions found in many situations. The first situation results when the hazard is miscalculated and the control measures then taken are too extensive and, of course, too expensive for the hazard involved. This is a situation of too much control which is often criticized by management and employees creating a poor climate of attitude and feelings for an effective fire prevention and protection program. The second situation again results from the miscalculation of the fire hazard and the control measures taken are weakened by consideration of operational factors and are not adequate for the degree of hazard involved. In this situation it is a case of not enough control, and a fire occurrence will be the ultimate result. Needless to say, this eventuality does not reflect favorably on the fire control and prevention operations.

The control of fire hazards must be evaluated for each specific hazard. The application of blanket rules to every fire hazard in a "canned" approach will result in the misconceptions we have mentioned above. The control of each fire hazard must be *evaluated, analyzed,* and *solved* as an individual problem in relation to the over-all safety philosophy of your industry.

The detection and control of fire hazards in industry CAN be accomplished by continuing our engineering and educational efforts, considering also the human situation which will determine the usefulness and effectiveness of these efforts.

FIRE PREVENTION EDUCATION, By HAL H. HOOD, *Fire Marshal, Dallas, Texas*

We have come a long way from factories of several years ago in which there were few, if any, fire protection facilities. In that day and time there were not enough aisles in storage areas, not enough sprinkler systems, not enough fire-seperation walls and fire doors. Buildings were made mostly of highly combustible construction and built too close together. The water supply was usually inadequate,, fire extinguishers were not provided in hazardous areas, etc.

In those days conflagrations were not uncommon. The Chicago fire, which was started by an overturned lantern, is just one example of the lack of pre-thinking about fire protection facilities, construction of fire-separated buildings, etc.

Our present day factories, in which fire prevention and fire protection start on the drawing boards, present quite a different picture to those factories of years ago. This is due to the efforts of many people. One group which has been largely responsible for bringing about these changes is the insurance underwriters—the people who have to pay the bills for these fires.

In our present day factories the water supply, pumps, underground mains, and sprinkler systems must be adequate to provide protection for the occupants. . Automatic protection devices and alarm systems must be provided for extra hazardous operations. Fire separation and access aisles must be provided. A good fire alarm system must be provided with a trained fire department, either on the property or close enough to provide protection. These and many other things we must provide, or else we pay a penalty in insurance premiums.

Yes, we have come a long way in fire protection "Know How." We have made great advances in fire-protection engineering. *BUT* our fire loss remains at much too high a level, and the number of people killed and injured in fires each year remain about the same. Why is this? What is wrong? Have we missed the boat somewhere? The fire-protection engineers know the answer to these questions, and so many professional firemen. In many modern industries the people in top mangement know the answer and are taking progressive steps to do something about it.

The answer is simply this. In spite of the many hazardous and dangerous materials which are handled in industry, the three greatest causes of fire are still men, women and children.

One way to bring down our fire loss and prevent death and injury by fire is to educate our people; to teach them what causes fire, how to prevent it. This sounds simple, but it requires the best selling job that has ever been undertaken. Most people either

think it can't happen to them, or just don't think at all. Something has got to be done to wake these people up, and make them realize that there is a need for them to learn what action to take, and to think about fire prevention every day. They have GOT to be made to think it can, and is likely to, happen to them if they are not careful.

Where do we start? How do we go about training our people?

Well, in most things we start at the bottom and work up, but in fire prevention education in industry we are going to have to start at the top and work down. Top management must believe in it. They must believe in it enough to put some money into it. They must let all under their supervision know that they are solidly behind the program. Without the backing of top management no successful education program can be carried out.

Next, we must plan an education program. All phases of fire prevention should be included, but each industry should take into account the most prevalent hazards of its particular industry and give these priority. Some of these we will mention.

Cutting and Welding: Close supervision by qualified persons should be maintained over all open flame operations. In regular welding areas regular inspections should be made to see that no flammable liquids or other combustible materials are used in these areas. When this type of work is done outside of regular welding areas, a written permit should be issued by a qualified person after an inspection is made and all necessary precautions are taken. These permits should be issued daily because of changing conditions and, if the job is moved a short distance, another permit should be issued for the new location. It is very worthwhile to write a *hundred* unnecessary permits in order not to overlook *ONE* necessary one. A good example of the hazard involved in such operations is the Lavonia, Michigan, transmission plant fire.

Handling Flammable Liquids: People who handle flammable liquids should be taught by means of demonstrations, films, lectures, etc. the hazards involved and the means of preventing fires and explosions. Also, these people should be trained in the use of extinguishers for Class "B" fires. Many agencies have flammable liquid demonstrations which are impressive and educational.

In case of a large concern with a great many people involved, it might be worthwhile to develop its own demonstration. If a physical demonstration is not available or practical, there are several good films on the subject. Whichever means is used, a schedule should be set up so ALL employees and particularly supervisors are included. Training in the use of extinguishers should include actual use of the extinguishers on fires by the employees.

Good Housekeeping: "A clean house seldom burns." This should be impressed upon employees. Trash should be put into proper containers and removed regularly. Aisles should be kept clear of obstructions. Fire doors should be kept unobstructed. Stock should not be piled too near sprinklers. These and many other good housekeeping practices should be so impressed upon employees that they are constantly conscious of them.

Fire Inspections: Regular inspections should be made by qualified persons. When hazards are found the inspector should explain why the condition is dangerous and what steps should be taken to correct it. Even though an inspector has the power to enforce action, he should try to sell the person concerned on the idea, so that person will believe in fire prevention and think in terms of fire safety. Any inspection program should have a follow-up system.

Volunteer Fire Brigade: It is usually best to have a professional fire department augmented by a volunteer fire brigade, but this is not always practical in small plants because of the expense. However, most plants CAN afford to have an organized volunteer fire brigade. A professional fireman should be employed to train the volunteer brigade. The purpose of such an organization is threefold. First, it places trained men in each unit to work for fire prevention. These men are close to the operations and can see and recognize hazards as they occur and can take steps to eliminate them. Second, if a small fire occurs, a trained man is nearby to extinguish it in its incipiency with the proper extinguisher. And third, in case of a large fire the fire brigade can supply trained manpower to assist the professional firemen when they arrive.

Training for the fire brigade should include the following:

1. Fire inspection practices.
2. Use of first aid fire extinguishers.
3. Extending hose lines from hose houses, hose reels, or from fire hydrants by hose carts.
4. Use of fire ladders.
5. How to assist professional firemen in laying lines with engines.
6. Use of forcible entry tools and ventilation.
7. Use of gas masks, respirators, and resuscitators.
8. Use of rope and fire department knots and hitches.
9. Rescue practices.
10. First aid.
11. How to deal with special hazards, or dangerous materials, peculiar to the industry concerned.
12. Location of sprinkler valves and how and when to turn them off on orders from responsible persons.

Orientation of New Employees: All new employees should be taught how to turn in a fire alarm, either by telephone or fire alarm box, and what steps to take after turning in the alarm. Also included in the orientation of new employees should be instructions not to smoke in prohibited areas, not to impair or block fire equipment, fire alarm boxes, hose reels, extinguishers, etc.

Fire Bills: Fire bills should be posted in all units, giving instructions for actions to take in case of fire. All employees should be required to know the location of fire alarm boxes, fire exits, etc.

Remember 90% of all fires are caused by people, only 10% are caused by things.

Part Two — THEFT

INVESTIGATION OF THEFT IN INDUSTRIAL PLANTS, By DAVID H. TROUPE, *Marquardt Aircraft, Inc.*

The best method of controlling property thefts is not by means of investigation, but by a good theft-prevention and control program. We do know these thefts occur despite our best efforts and, therefore, must be prepared as a part of this program to institute an investigation. What, then, is the most desirable climate for a successful investigation?

Industrial Security or Plant Protection Departments can render a valuable service to the employee and the company by investigation of thefts and recovery of the missing items. The apprehension of a thief acts as a deterrent to others and contributes to the prevention of further thefts. Investigation resulting in the location of mis-routed property can provide a basis for a change in procedures which will prevent a recurrence of similar incidents with resultant savings in time and money to the company.

Several factors operate in an industrial organization which tend to make investigation of incidents relating to the disappearance of property difficult. The failure to report such incidents promptly to the Industrial Security or Plant Protection Department hinders investigative efforts. Complex problems are encountered by many organizations in the establishment of adequate inventory controls, means of marking company or personal property, etc., due to the large number of personnel or decentralized facilities. The physical lay-out of many industrial plants makes it impossible to conduct a physical surveillance. The use of technical or other investigative aids such as the polygraph, paid under-cover agents, etc., may be prohibited by company policy. The fear of industrial organizations concerning civil suits and their distaste for adverse publicity sometimes influences the application of investigative techniques to the solution of incidents.

I wish I had some magical formula for you to use. I wish I had a new type crystal ball to give you, but I'm afraid I can't. There is no substitute for painstaking work and adequate preparation for solving these cases. Therefore, I'm simply going to outline some basic fundamentals to keep in mind and, if practiced, they frequently pay off.

I think the first thing is to agree on a policy with your own mangement as to what happens to a thief when caught or when evidence is developed indicating his guilt to a reasonable degree of certainty. Nothing is more discouraging to a professional investigator than to see the results of his work go for nothing. Therefore, by agreement with your management, the penalty should be swift and final.

cution. This, again, is a policy decision on which many companies do not agree. In the establishing of a theft investigation program, the following points

I am not going into the problem of firing and prose-should be emphasized: (1.) Prompt reporting of thefts or missing property. (2.) Immediate investigative action on such reports and the application of specialized investigative techniques to the follow-up investigation.

Failure to report incidents promptly allows evidence to disappear, records to be lost or misplaced, witnesses to forget essential details and suspects to gain time to think up explanations for their activities or provide a convenient alibi. A management and employee educational program built around articles in the plant paper and meetings with supervision by security personnel designed to improve reporting practices will materially assist in minimizing the problem.

An adequate preliminary investigation conducted immediately after the report of the theft or missing property is essential to the successful follow-up investigation. A thorough inquiry made at this time accomplishes several objectives. If there is physical evidence which indicates that a theft has been committed or that a forced entry had been made, the preliminary investigator can properly preserve the evidence from further contamination. He is in a position to keep unauthorized people from handling evidence that would be valuable to the investigation. A good impression is made on the victim or company representatives. They will know that every effort is being made to apprehend the thief. An adequate investigation at this time can determine certain basic facts which may prevent the investigator from developing a wrong hypothesis relative to his course of future investigation. This results in the saving of time and in many cases will enable the investigator to satisfactorily bring the case to a speedy conclusion without having to retrace his steps.

As a general basis for the investigation of thefts and the location of missing property, the preliminary or follow-up investigator will find it profitable to record some of the following data in the initial stages of the inquiry:

a. The date and hour of the theft.

b. A complete list and description of the stolen or missing property. If the victim or custodian of the property is unable to provide serial numbers or identification marks, there may be several witnesses who can offer a description of the property. This information should be obtained independently from each witness.

c. Location of the property at the time of theft and other locations where the property had been previously stored, and various searches for the missing property.

d. Determine reasons for placing the property in the location it was at the time of theft.

e. The identity of the person who first discovered the loss. How did it come to his attention? Was he the logical person to make the discovery? Who would have automatically made the discovery? Are there any other witnesses to the discovery?

f. A list of persons who knew the location of the property or the existence of said property.

g. A list of persons who had access to the property.

h. Duties and movements of persons having access prior and subsequent to the discovery of the loss in cases where the time interval is reasonably short.

i. Ownership of the property—company, personal, government.

j. Physical evidence such as latent fingerprints, shoe prints, tool marks, articles of clothing or similar traces left at the scene. This is highly important where there is evidence of forced entry.

k. Suspects named by the person having property in his custody. Reasons for his suspicions.

l. Character of property, saleability, uses, etc.

m. Reconstruction of the theft or loss; means of access, if any; selection of time. Was there a *modus operandi* to the theft or loss? Was there a method used to conceal the theft or loss?

The investigator who receives a report of a theft or missing property where an adequate preliminary investigation has already been made should reinterview the victim or the custodian of the property. This person may have additional information. Unless there is definite physical or verbal evidence of forced entry or theft, the investigator should at this time determine the following facts:

Trace the movement of the property at its original point of entry into the plant to the point of disappearance. Was the material or item involved actually brought into the plant? When? What happened to it? Who received it? What papers were signed proving that it entered the plant? If material, was it placed in the storeroom or stockpile?

If it consisted of company tools, did they actually get into the tool crib? If personal property, when and where did victim purchase it? When did he bring it into the plant? When did he last use same? Has he ever loaned his property for use to ther persons?

The steps enumerated above, in many cases, will result in the recovery of the property with the discovery that it has been simply misrouted or mislaid by some employee. If tracing the movement of the property does not result in a recovery, the follow-up investigator can adopt a reasonable conclusion that it has left the plant premises. A list should be made of the possible markets for the disposal of the property. Could the person in custody of the property or the victim be a logical suspect? In many cases a theft is simulated by the victim to cover up a false insurance claim. The investigator should determine what person having access to the property would have the best motive for taking the property. This can be determined by any of various methods.

Interrogation, in many cases, is the only means whereby an investigator can bring the case to a successful conclusion. The only evidence pointing toward the subject in question may be the word of an informant. There is no physical evidence to connect him with the theft; he has no criminal record; has a good work record and is only one of many who had access to the area from which the property was found missing. It, therefore, behooves the investigator to learn the techniques of interrogation and the various approaches that are used to obtain information from persons suspected in a case.

The following forms of instrumentation have been used very effectively in apprehending suspects engaged in thievery in a particular area or location within the plant:

Powders and dyes can be placed on objects and used as traps in areas where thefts have been occurring. They can also be used on surfaces which a suspect might touch. The powders and dyes are carefully dusted on pocketbooks, wallets, drawers, door knobs, on any other objects which the thief is likely to touch. If the thief takes only one type of object such as money or candy from unlocked desk drawers, this type of property should be dusted with a powder or dye and placed in likely areas where the suspect might look.

Dyes can be obtained in the form of a powder or paste. When the suspect touches an object covered with the powder or paste it will be transferred to his hands or clothing and will result in a stain appearing. The powder or paste is usually selected for the permanence of its stain and for its color. A color should be used that is similar to the object upon which it is placed. The following are some of the powders and pastes which have been found usable:

Name	*Color Dry*	*Color Wet*
Chrystal Violet	green	violet
Chrysoldine	maroon	orange
Malachite Green	green	green
Methylene Blue	dark green	blue
Rhodamine B	brown	cherry

All of these dyes can be removed by persistent washing. In their use some provision should be made by the investigator to apprehend a likely suspect as soon as possible after he has touched the object or area that has been prepared.

Sirchie Criminal Research Products, Inc., produces a silver nitrate dust that can be used for the purposes enumerated above. Objects which have been dusted with this preparation cannot be handled without picking up its incriminating stain. The dust sticks to the skin and the natural oils secreted from the body cause a chemical reaction which produces dark brown specks that positively cannot be washed off. The speck or stains will remain on the skin for no longer than 7 days, all fluoresce under ultra-violet radiation. They should be used in small quantities. The powder or paste can be detected by the suspect if an excess amount is placed on the object or area that is used

as the trap. The following powders and pastes have been found to be effective:

Name	*Visible Color*	*Ultra-Violet Color*
Fluorescein	maroon	yellow
Rhodamine B	brown	orange
Uranyl Nitrate	yellow	yellow

Invisible inks—inks that can be used on any material and will not be harmed by water—can be applied by a pen, brush, spray, or injection with a hypodermic needle and can also be used on leather or the inside of fur pelts. This type of invisible ink will fluoresce under ultra-violet light. An "invisible" crayon, with which the investigator can mark certain objects to fluoresce under ultra-violet light, can also be obtained. Marker Lac, manufactured by Glowspar Co., fluoresces under black light. It allows for invisible markings to be placed on metal, plastic, wood, etc., and is applied with a brush.

In areas subjected to extreme weather conditions such as rain, etc., where there is a strong possibility that the powder or paste may be washed off, the following method may be used: A saturated solution of Crystal Violet or one of the other stains mixed with olic acid "red oil" and placed on the object that the suspect is likely to touch. It should be placed on the object in a position which is not in the line of view of the suspect.

In thefts of gasoline or other soluble liquids certain chemicals can be added to the substances which later on can be detected through a chemical examination of samples taken from the suspected material found in the possession of the suspect. An amount equal to 56 milligrams phenolphthaliane is used for each gallon of gasoline. To detect the phenolphthaliane a sample is taken from a suspect's automobile tank or container in his possession. One cubic centimeter of a 5% solution of sodium hydroxide is mixed with ten cubic cm of the gasoline. If a red layer is observed at the bottom, the gasoline contains phenolphthaliane. Fluorescent substances can also be used in the detection of thefts of gasoline or other soluble liquids. A tablespoon of fluorene or anthracene powder added to a 500 gallon tank of gasoline will cause samples of the gasoline to fluoresce under an ultra-violet lamp.

The use of photographic methods for the apprehension of persons suspected of committing acts has been adopted by law enforcement agencies throughout the country. The adaption of this media to industrial security investigations has enabled these organizations to solve many difficult cases and at the same time result in a substantial saving in cost. Recurring cases involving small amounts of property do not always lend themselves to the use of other techniques in the apprehension of a suspect. This is particularly true in large industrial organizations. The articles taken may be from an area to which a hundred or more people have access. The type of article taken may be only one of many hundreds that are similar to it in appearance. Under these circumstances the use of other forms of instrumentation, surveillance, and additional follow-up investigative techniques are not the most practical methods for bringing the case to a successful conclusion.

Cine-Kodak Model K-100, 16 mm camera may be fitted with a device known as an "intervelometer." This device allows the camera to reproduce a sequence of pictures at spaced intervals. The device is actually a Bristol motor which can be purchased at a cost of approximately $3.45. The motor can be operated 1/15 rpm to 20 rpm. The motor actuates a trip on the camera which can be set to trip the camera at regular intervals depending upon the needs of the operator. The timing device can be adjusted to record a picture every five seconds or every thirty seconds, etc. The standard roll of film approximately 400′ in length used with a K-100 camera records at 16 frames per second and the film would be expended in approximately four minutes. For the timing device set at five second intervals the same roll of film will cover a period of eight hours.

The camera may be concealed in a small box with false mirror in the front which allows the camera to reproduce pictures through the mirror. The camera and equipment as mentioned above will record pictures in an area covering approximately 600 to 700 square feet. The camera and timing device may be connected with an electronic eye or infra red detection device. These electronic eyes, as they are commonly called, emit an invisible beam across a certain area. A person, by crossing the invisible line, breaks the beam and sets off the actuator on the timing device. The timing device in turn starts the camera in motion and reproduces pictures at the desired intervals as prearranged by the operator of the camera. Telescopic lens can be attached to the motion picture camera and used with the timing device. Tests with a 6-inch telescopic lens reproducing pictures at a distance of 500 feet disclosed that a figure that could hardly be discerned with a 1-inch lens at the same distance could be clearly identified with the use of the 6-inch lens. The 6-inch telescopic lens can be used to distances up to 1000 or 1200 feet.

The primary use of the time sequence motion picture camera is for the purpose of identifying a person or persons who are engaged in suspicious acts. Due to the spaced interval it is rare that a person who appears in the photograph will be actually committing an illegal act. However, the time sequence shots may disclose a suspect in the act of opening a desk drawer from which articles are missing and five seconds later another photograph will disclose a man walking away from the desk. The photographs will assist the investigator in identifying the person who could be the logical subject for interrogation purposes.

Still cameras, motion picture cameras or the time sequence camera can be used for taking photographs at night. In areas where there is poor reflected lighting an extra fast film should be used with the camera. The Eastman Kodak 52-78 Tri-x film used with a high speed development process is quite effective in obtaining clear photographs under the foregoing circumstances. Tests that have been conducted disclose that on a moonlit night this type of film will record objects clear enough to be identified.

The use of infra red film with the different types of cameras generally necessitates the addition of some type of infra red illumination. Complete darkness or poor lighting in themselves do not provide sufficient infra red rays. Infra red bulbs are used by photographers to provide the necessary infra red rays. These emit a red glow and can be seen by the naked eye. The amount of infra red radiation that can be provided by this method is generally limited to a very small area. In most cases involving the use of infra red film for illumination a still camera would be used for the recording of pictures. A camera using infra red film and fitted with infra red flash bulbs can be actuated by means of an electronic eye as described above. Infra red photography has been found to be useful mainly in cases involving small, tightly secured areas that are being entered surreptitiously.

Latent fingerprints, tool marks, etc., are difficult to obtain at the scene of a theft committed in a large industrial organization. In those circumstances where prints are most apt to be found, such as the smooth surface of a desk, large numbers of people generally have access to the area where the theft was committed. Dusting the surface for latent prints under these circumstances may provide numerous impressions which could be identified with a suspect if his identity were known. Other locations in an industrial plant from which property may be taken do not usually provide surfaces receptive to the impression of a latent print.

However, industrial security division units should have in their possession equipment needed to develop and process latent fingerprints. The appearance of an investigator at the scene of a theft with fingerprint equipment may be of great psychological value in bringing the case to a successful conclusion. In many cases, even though a good print cannot be obtained, the suspect whose identity may be later determined through follow-up investigation or informants is not aware of this.

Investigators should be familiar with what the laboratory provides in the way of service to them. Industrial security units should have access to scientific crime laboratories for the examination of other physical evidence that may be found at the scene of an important theft. This will include footprints, tool marks, etc.

PREVENTION AND DETECTION OF THEFT IN INDUSTRY, By E. A. SCHURMAN

Bell Helicopter Corporation

Let's break this subject down into four parts:

(1) Dollar Loss of Pilferage and Theft
(2) Methods of Pilferage and Theft
(3) Prevention
(4) Detection

The problem of pilferage and theft is common to all industry. There is not an organization repesented by our membership which does not suffer a substantial annual loss from theft. The dollar value of this loss, is, of course, in ratio to the number employed, the effectiveness of material and equipment control systems and the efficiency of the Security Department. The type of product manufactured and the nature of inventory items available to employees will also affect the annual loss.

It is generally accepted that all thievery cannot be stopped even with the best of systems and the most efficient security personnel. As a matter of fact, the cost of implementing a foolproof system or of providing sufficent security personnel would, in the case of many companies, far exceed the value of the potential loss. It is certain, however, that the enormous losses experienced by industry, currently estimated at 500 million to 2 billion dollars annually, can be substantially reduced by those companies who take appropriate steps to prevent and detect pilferage and theft.

Before discussing how we can prevent and detect our losses, we should first consider what items go to make up the loss experience of our companies and WHEN, WHERE, HOW and WHY these losses occur. We must also define pilferage and theft. Certainly, we cannot classify as a thief the office worker who inadvertently takes a pencil home—but, what about the employee who at the beginning of the school term equips Junior with a supply of company pencils, notebooks, paper pads, ink, and other standard office supplies and who replenishes these supplies as needed throughout the school year. What about the Scotch tape that goes out for use as wrapping for Christmas gifts? Or the employee who takes four bolts and nuts with washers to mount his new automobile licenses? The cost of these supplies may be small when considered individually, but when multiplied by the hundreds, represent real money. It may be that we should not consider these losses as a matter for consideration by the Security Department, but certainly a substantial saving can be affected if these practices can be stopped. There is no question as to how we should classify the individual who systematically accumulates a well equipped home workshop, at the expense of the company or those employees who remove items large or small and convert them into money.

Obviously the problem will differ with each company or facility. The theft of such items as drills, small hand tools, nuts, bolts, Scotch tape and pencils which can be concealed on the person is more difficult to prevent and detect than the theft of sheet steel or aluminum ingots.

A typical illustration of what industry is losing involved a painter who had a thriving business on Saturdays, Sundays, and holidays, using materials stolen from his employer. Paints, lacquers, thinners, and

linseed oil were removed at the rate of one quart a day in his thermos bottle.

There is one classic case of record where a female employee took one roll of toilet paper each day over a long period of time. An extreme in the other direction was a case involving the theft of $10,000 worth of major aircraft components.

The toilet paper was concealed on the woman's person. The aircraft parts were removed in the trunk of a trusted foreman's car who was permitted to park inside the perimeter fence. Another case involved a tool crib attendant who over a period of one year stole $1,500 worth of drills, taps, reamers, dies, etc. Most of these items were taken out in his thermos bottle from which he had removed the glass liner. Packages of one dozen high speed drills were placed in the back of a partially used package of king size cigarettes. Longer and more bulky tools were concealed under his shirt and trousers, held in place by his belt and secured to his legs, forearms, and body by friction or masking tape.

One company which uses an exchange system in their tool crib which permits an employee to trade a broken drill for a new one upon the surrender of the shank end of the broken drill (only the original issue is made a matter of record) noticed that there were periodical runs on the tool crib for new drills. Investigation disclosed that the tool crib attendant threw the old drill shanks in a bin under the counter and when it was full, dumped them into a trash can. Employees observing this practice, picked out the drills by the dozen and again exchanged them for a new one. These drills then left the plant.

These methods are well known to all of us and can logically be called the "Unassisted Method," Such thefts occur at the time the employee leaves the premises whether it be at the end of the work day, at lunch time, or any other occasion he has to leave the plant.

Many ingenious schemes are employed in what I like to call the "Assisted Method" which frequently involves more than one employee. We can include in this category: (1) material thrown over the fence to be picked up immediately by a second person or recovered later, (2) items placed in waste containers and salvaged from dump areas, (3) items placed in vehicles operated by the Company, outside vendors or subcontractors, and unloaded outside the plant, and (4) material and tools sent to the Salvage Department as worthless, and later purchased as scrap by employees or junk dealers. Forged removal passes and dummy paper work can also be used effectively in removing material from the plant.

Not many months ago at one company, a load of 30 sheets of four foot by eight foot 3/4 inch plywood was removed with legitimate paper work. There was no failure on the part of the guards at the gate as all paper covering this shipment was in order. The theft would have gone undetected had it not been for an informant. The procedure was simple. A shipping clerk was in collusion with a truck driver. The clerk prepared a set of Material Transfer Orders, shipping the plywood from one plant to another. Instead of processing the original copy of the shipping order which would have provided the record that the shipment had made, he destroyed it. After the plywood had been disposed of, the truck driver disposed of the papers attached to the shipment which normally would have been signed and processed as evidence that the shipment had been received. The end result was no paper work to evidence the shipment.

Let us consider this question—WHO WILL STEAL? —That depends upon our interpretation of theft. If we go back to the subject of pencils, Scotch tape, and bolts for license plates, it appears that the percentage would be staggering. There seems to exist among a great percentage of employees a philosophy that it is no sin to take small items or quantities of company property. People who would not think of stealing from anyone else will steal from the company for which they work.

On this subject, let me quote from an article by B. W. Gocke which appeared in the May-June 1958 issue of "Police." Mr. Gocke states, "As a matter of fact, it is the trusted employee who is usually found to have committed the largest thefts and embezzlements. The trust which has been placed in him by management puts him in a unique position to carry out his thefts relatively easily over an extended period of time . . . .

"These people who work in the plant day after day are the ones to whom the most attention should be given. They are the people who have ready access to the premises. They are familiar with the physical set-up of the buildings and grounds. They know the procedures, the supervisors, and the guards. They know which things are important and valuable, and they know the soft spots in the organization. In short, they are in the best position to know not only the location of articles of value, but also the best possible means of obtaining them. Moreover, as employees with daily access to the premises, they can proceed to make plans and take whatever steps are necessary for the acquisition of what they want."

The entire article from which these quotes are taken is well worth reading.

WHAT DO PEOPLE STEAL?—To put it bluntly—anything for which they have or can find a use or for which there is a market. Most of our losses dollarwise result from the theft of small hand tools and small quantities of supplies and materials which can be removed by an employee unassisted.

Although the material stolen and the manner of theft may differ, our problem is the same. HOW DO WE STOP IT?

To prevent theft, good control systems for material and equipment are, of course, an essential support to the Security Department. However, there is no question but that the two most effective deterrents to theft are (1) the shake down of employees as they leave the premises, and (2) a firm company policy that dismissal and prosecution are the penalty for theft. Unfortunately, for one reason or another, some

Security Departments are not permitted to make a personal shake down of employees. Those Departments that have this prerogative are indeed fortunate and should guard it zealously. The policy of immediate termination for theft with prosecution following, is more general. To be effective, it must be applied without favor. The employee with ten years of service should be terminated as quickly as the employee with a few months of service. There is nothing that travels faster than the word that someone has been fired for stealing and it is generally conceded that thefts subside for a time as a result.

Prevention of theft really starts with pre-employment screening followed by a good investigation by the Security Department during the employee's probationary period. These efforts will not prevent employment of someone who will steal but will certainly eliminate many thieves and other undesirables. The routine investigation of prospective employees has become standard practice with many companies. It is no longer necessary, even in the defense industry, for the Security Department to justify the expense. It is no longer a question of whether or not the individual is a good security risk from the standpoint of national defense . . . the question now is simply, "Is he the kind of a person we want working for the company—mentally, physically, and morally?"

The detection of theft comes after the fact. Detection picks up where prevention leaves off. Actually in our business, the two terms are largely synonymous. The shake down certainly has its effectiveness as a prevention and also serves as a method of detection. The same applies to material control. Records may provide proof of the guilty employee.

At Bell Helicopter, inter-plant shipments are now made in closed and locked van-type trucks. The pad locks on these trucks are all keyed alike and the guard at each truck gate at each plant has a key. No other personnel hold keys. When a truck checks out of the gate, at any plant, the guard unlocks the padlock which has been fastened in the staple of the hasp and locks the truck. When the truck enters the gate at its destination, the guard unlocks the truck and relocks the padlock in the hasp staple. In this way, trucks are unlocked at all times when inside the plant area and locked at all times when shipments are in transit. No inspection of the truck or load is made entering or leaving the plant—none is necessary. Locks and keys are changed at intervals as added precaution against compromise of the system. This procedure has completely eliminated (1) all thefts from shipments in route, (2) the use of this type of company vehicle for the illegal removal of material, (3) hundreds of investigations by the Security Department involving alleged thefts and losses of material in transit. There can be no argument if the material does not arrive . . . it was not shipped. While this system was installed primarily as a security measure, it has also resulted in tremendous savings in paper work for the company.

We should not ignore the matter of informants. It's an old adage that no police organization is any stronger than its source of information. It's surprising the number of people who are not only willing but anxious to contribute information to the Security Department provided they do not become involved. There seems to be a little of the "Dick Tracy" complex in most everyone. If properly encouraged on the basis of loyalty to the company, many employees will report that a theft is being planned or has been committed. Such sources of information should be encouraged. The case must be developed in such a manner that it is unnecessary to divulge the source of information.

Time will not permit us to go into a lengthy discussion of the many mechanical devices available to us such as closed circuit television, high frequency alarm systems, time sequence motion pictures, electric eyes, electronic fences, balanced electro magnetic field, metal detectors, and fluoroscopic devices such as inspectoscopes. The fact this equipment is known to be in use tends to prevent theft and their efficient use is a means of detection. It will be interesting to hear from the floor the experiences of those who have any of these devices in use.

It is unnecessary to go into details of standard control systems such as pass out for employees during working hours, material and package passes and truck passes. It is worthy of mention, however, that where some form of paper work is required for everything leaving the premises except lunch boxes and personal clothing, and the employees are aware of this fact, it is less difficult to establish the intent to steal, and to apply a policy of immediate termination for theft.

Those companies who—properly investigate employees before they are hired, or during their probationary period, maintain adequate control systems for material and equipment, an adequate guard force equipped with the tools to do their job—and rigidly maintain a policy of termination and prosecution as the penalty for theft——go a long way in combatting their annual losses from pilferage and theft.

WORKSHOP/SEMINAR VIII

THE EFFECTS OF COMMUNISM UPON THE INDIVIDUAL

An Address By MAJOR WILLIAM R. FEDOR, USA, *Industrial Personnel Security Review Division, Office of Security Policy, Department of Defense*

My first reaction to the invitation to talk to your Society on this topic was similar to what it would have been had I been asked to speak to the New York Yankees on "How to Win a Major League Pennant." It would be presumptuous of me to attempt to evaluate all of the aspects of this matter for, in the final analysis, the theme selected for Workshop VIII is basic to the problem with which world communism confronts us. If we understand the compelling effects that the communist system has upon the individual personality, we will know, in a large measure, communism's principal operational technique.

Communism, both in theory and practice, operates to achieve the complete negation of human individuality. It ruthlessly seeks to eliminate the innate desire of the human personality for freedom and attempts to substitute in its place resignation to the idea of a collective society. Communism is designed to weld the individual permanently and inextricably into the amorphous mass of those blindly following its dictates.

Certainly the basis of Western civilization, as we know it, is the principle of freedom of choice; the recognition that the indvidual has the sacred right to life, liberty and the pursuit of happines. Communism assaults frontally this cherished principle—for unless it can dominate, subordinate, and collectivize the individual, and in fact, destroy individual liberty, there would be little prospect of communism achieving its totalitarian ends.

We have this from no less an authority than Stalin himself, who said, "... for without the manhood, without the ability to overcome, if you like, one's self-esteem, and subordinate one's will to the will of the collective, without these qualities, there can be no collective, no collective leadership, no communism."

In discussing this subject it is necessary to narrow the scope of the discussion to the effect of the communist system upon the individual Communist Party member. It is the individual party members who form the dynamic core from which communist action radiates and who, in turn, control the mass organizations which serve as transmission belts over which the Party's influence is disseminated.

The actual number of Communist Party members, to be sure, is slight in comparison with the terrific consequences resulting from the Party's subversive efforts. Let us then consider how this numerically small organization is able to accomplish what it does.

The basis for the communist organizational structure is revealed to us in a pamphlet written in 1902 by Lenin and entitled "What is to be Done?" Lenin argues that the goals of world revolution can only be attained by a small hard-core elite of professional, thoroughly trained and highly disciplined revolutionaries. Thus; in spite of all the slogans designed to attract mass support, Lenin, years ago, determined that the Party itself should not be a democratically organized movement. The so-called "vanguard of the proletariat" would be a closed door proposition, the admittance to which should be limited to a chosen few who would submit themselves to absolute control from above. And, paradoxically, the hard core of the communist movement is composed of intellectuals, not of industrial workers. A few functionaries at the top exercise control over the party echelons which spread out in a pyramidal fashion below. Thus, the key to Party "unity" is discipline—total, complete, unswerving, unquestioning discipline. This, in communist jargon, is known as Democratic Centralism.

The communist initiate is promised that for his efforts in behalf of the Party he will be rewarded with a better world—indeed—a perfect world. This is an appealing objective! Now it should be recognized that many who take the Party vows are deluded into honestly believing that they are working for the improvement of society, for freedom, for justice, for progress and the full expression of man's talent and ability. They are assured that the fulfillment of man's desires is to be found in Marxism-Leninism. This claimed capacity of communist doctrine to be both a key to the understanding of the past and present, and at the same time a guide to future action, is of decisive importance in the indoctrination of Party recruits. Thus, armed with the "infallibility" of its dogma, the Party promises to lead the exploited and downtrodden toward the rebuilding of society, to the full realization of human nature and, therefore, to the "freedom" of the classless society.

There should be no mistaking the tremendous impact that the communist ideology has had—and continues to have—upon the world.

Wladamir Gurian, noted political analyst, advises us that among the reasons today for communism's great influence are: (1) it is backed by the experience of the successful conquest of a great empire and, (2) communism is grasped by many, not in its effects, but only in its promises. These promises make the existing conditions look darker than they really are, and the coming of Bolshevism is compared with the imperfect reality. Thus, in the name of the coming perfection everything which promotes its coming is permitted. Intellectuals are attracted by this political secular religion because it gives them certainty and calls for activity, and the masses are seduced by its role as the destroyer of injustice and imperfections. The intel-

lectuals do not realize that the Bolshevistic certainty is based upon the whim of political powers who interpret the doctrine according to the needs of the totalitarian control, and the masses are unaware that Bolshevism, when victorious, replaces existing imperfections with a system which is infinitely worse than the imperfect conditions of the present.

Consequently, the Party strives to impress upon its members the desirability of the promised end, thus paving the way toward getting them to accept the means. Any and all means to achieve the promised end are, to the communist, ethical. The Communist Party is at war with the rest of society. It is pledged to destroy society as we know it, to rebuild it in the image of Maxism-Leninism. There is no compromise in this war! The communist is taught that his enemy is ruthless, merciless and unprincipled. Accordingly, to defeat him the communist is justified in being more ruthless, more merciless and more unprincipled. And in this connection, the hardened communist has no qualms of conscience insofar as unethical action is concerned.

Test this for yourself. Question any open communist on the ethics of his behavior and he will not attempt to defend himself. Rather he will cite where in his opinion "the present system" has been just as unethical. He has an end in view. The establishment of a communist society. That to him is a good end and everything that hastens it, however bad in itself, is a good thing. This type of rationalization characterizes communist thinking from the rank-and-file fanatic to the key officials of the Soviet hierarchy. Continuing examples of such rationalization may be found in the foreign policy of the Soviet Union today. In this connection, you will recall that the Soviets went to no great length to defend their brutal repression of the Hungarian revolution; rather they accused the West of inciting revolt and used similar false accusations and distortions in an attempt to shift blame.

Therefore, it is important that we understand such "irrational rationalization," if I may use an anomally, for this is basic to the communist dialectic. And once an individual succumbs to the Party's philosophy, he has placed his normal thought processes in great jeopardy. For when a person gives himself to the Party, it must be all or nothing at all. His conscience is placed in pawn to the Party, and he is taught that there is no middle line. Marxism preaches the inevitability of revolutionary change within society. Anyone who does not fully acccept this is working against the communists, and for this reason, Party indoctrination is a process directed toward total acceptance.

The effect of Party indoctrination cannot be better described than it has been recently by J. Edgar Hoover, who says, "Communist members learn what to think, how to vote, what to say, by a process of 'automatic osmosis'—the seeping of pre-digested thoughts along the Party line into all subordinate minds disciplined to accept. The members become ideological sleepwalkers, drugged into complete obedience by an unconscious discipline . . . That is why the Party keeps stressing Marxist-Leninist education, Party schools, reading the Communist Press, self study. It builds a discipline that automatically attacks doubts, rationalizes contradictions inside the Party structure, and guides every decision in the Party's favor."

The "mature" communist must be able to submit his memory and judgment, his senses and their evidence to the superior mind of the Communist Party. If the dictates of the Party contradict his memory and the evidence of his senses he must nevertheless be able to believe the dictates of the Party with sincerity, passion and conviction.

Party discipline pervades the Party member's entire being, his every action must be taken conscious of the Party's desires. He can never be forgetful of his obligation to serve and that the Party has a job to be done whether he be at home, at work, at school, or, if he was once a believer, even within the Church. One former member of the Party explains that over a long period and through a slow process of constant discussion, schools and self study, the Communist Party builds a conscience of responsibility upon which it then relies to keep a member functioning, even though any real desire to do so has passed.

The effect of communism upon the individual member's home life is fundamental. There can be few communists with a happy home life. For the essence of family relations is tolerance. The essence of Party work is intolerance. The Party instructs its members to be free from family trouble. A member whose wife or parents oppose his way of life is a potential danger to the Party. He is instructed either to recruit his family into the Party or to leave them, if they interfere. There can be no compromise. He is taught to believe that those of his family who do not share his beliefs are dupes of the capitalistic system. The stronger his family's opposition becomes, the stronger becomes a communist's hatred of his family.

The communist is a man who lives on hatred. He soon believes that everybody's hand is against him. He trusts no one who is not on the Party line. Even his family! The Party takes charge of his conscience and his affection. This total demand often produces severe inner turmoil within the Party member.

In this connection, consider the testimony of an industrial psychologist, familiar with communist techniques, testifying before a congressional committee.

"Torn between the devotion to the Party and his [the Party member's] basic, though perhaps subconscious, devotion to his family, frustration develops . . . which could produce a condition of neuroses . . . Communism is his first duty; his family life is not really respected or given consideration . . . it is a battle between the innate emotions of family on the one hand, and of a fanatic idealistic existence on the other . . . the completely fanatic communist may arrive possibly at some sort of abstract happiness, but even so, he will continue to suffer for his entire existence because that abstract happiness is in conflict with his innate emotions and family relationship. In brief, the only possible basis for adjustment can come within the family itself, and this means quite clearly that happiness cannot lie in the direction of communism."

All of us know that education is a great instrument which may be used either to strengthen or weaken our free society. The Soviets have long recognized that in subverting a nation such as the United States, infiltration of the educational process is of prime importance. We know that the communists have made the penetration of schools and colleges one of the major considerations in their psychological warfare designed to control the American mind.

The effects of the Party's subversive efforts upon individuals active in the field of education have been charged clearly by the testimony of many ex-communists before Congressional committees. Thus, we learn that students are conditioned to hate their parents, to rebel against their leaders; to regard elders as enemies; to be filled with contempt for tradition, authority, and culture. Teachers in their turn are incited against "the ruling class' which exploits them. They must be filled with rebellion and hatred; this must be directed against the public, the parents of the children they teach, and the "class" that enslaves them.

These are strong words, to be sure. However, the record speaks for itself. We are aware that communist objectives in this area are pursued with a subtlety of approach that camouflages the true purpose of the conspirators. The nature of the conspiracy is well illustrated in the Party press which for years has pointed out that "Maxist-Leninist analysis must be injected into every class" and that "The Party must take careful steps to see that all teacher comrades are given thorough education in the teachings of Marxism-Leninism." However, the Party cautions that this infiltration and agitation must be accomplished in such a manner so that the infiltrators will not "expose" themselves. Similarly, the ideological training of Party recruits in colleges and universities is accomplished in carefully controlled increments, and in many cases, only after a considerable time has elapsed does the individual begin to realize he is trading his freedom for communist promises.

". . . Many of these individuals joined the Communist Party without knowing exactly what they were joining. They joined because they thought it meant freedom of speech, because they thought it meant a fight against discrimination, or a fight for better teaching conditions, or a fight for better conditions for children. Most of the motives for which they joined were good motives but what they got into was something which proved to be contrary to any of the principles that they held.

Soon they were abruptly confronted with the fact that a member of the Communist Party cannot hold "any" ideas. Rather he is obliged to hold *certain* ideas. Thus, in joining the Party he has submitted himself to thought control of the most rigid order. Any ideas or concepts which he previously held and which he now finds to be in conflict with Party dogma must be obliterated from his mind.

The forcing of Party members to walk communism's ideological tightrope often tends to produce a psychological disturbance within the individual, for communism represses the individual in his natural search for truth. The individual is forced by the Party to accept its dogma, its explanations, and its answers, even though these may fly in the face of obvious reality. The Party member is obliged to practice not only deception, but self-deception. This makes membership in the Party a constant challenge, and eventually the member becomes consciously aware that he, personally, is practicing self-deception. There is a direct connection here between this phenomenon and the widespread suspicion prevalent among Party members—suspicion of each other. For undoubtedly, their own motives unconsciously add to that quality of suspicion. Their adherence to communism, ostensibly so idealistic and in reality so much a product of their own emotions, does not bear up under their own scrutiny while they are in the Party. Why should they think that, in this respect, other comrades are any better.

This is really the central aspect of communism's effect upon the individual. It is the constant pressure upon the individual to relinquish personal control over his conscience. Any creative inclinations within him, unless they conform to the Party's desires, must be stifled. He must fit himself into a rigid and explict program.

Adherence to the Communist Party discipline makes particularly significant demands upon the American for he has experienced and enjoyed the basic freedoms characteristic of our way of life. To be sure, the average American finds himself involved in a variety of environmental associations, each one setting forth its ideals and each one making its claims for loyalty in varying degrees. However, he may without great risk engage in a certain amount of picking and chosing without provoking severe sanctions. And in his political affiliations, his social relations, and his recreational life, he is not required to make binding committments to exclude ideals and obligations. In fact, because the various groupings and social elements compete with one another for his loyalty and adherence, there is a very real sense in which he is master and can make his own choices, as well as fulfill demands which are in good part a matter of his own decision.

However, in contrast to the multiplicity of models confronting men in our or other Western societies, the communist movement confronts its membership with an exclusive and explicit model. This model is structured upon the ideological pronouncements of Marxism.

The model may not be and, very frequently, is not freely visible at the point of recruitment, as we have already said. However, once drawn into the Party, the novice is exposed in varying but ever-increasing degrees to this explicit model of the communist militant.

Once this self-image is incorporated, it establishes certain set ways of viewing the self and others, of appraising situations, and of organizing behavior, from which escape is costly and difficult. The painfulness of this process of escape, however, is to be attributed not only to the fact that an individual has assimilated a highly elaborate code of conduct and now has to re-

ject it, but also to the fact that this has become his only code and that now in a very real sense he has to destroy this self and find a new one.

But to imply that the effect of communist indoctrination upon Party members is so complete and so irreversible is to assume a defeatist attitude and certainly reflects inability to discern one of the weakest links in the chain with which the Party enmeshes its member.

The constantly swelling ranks of defectors from the Party attest to the Party's failure in its attempt to "straight-jacket" human thought. It is significant that looming large among the reasons given by ex-communists for their defection is this unacceptable threat to their individuality.

Even the most naive of individuals, no matter what his personal motivation for joining the Party, experiences sheer agony when he attempts to honestly rationalize the "zigs and the zags" of the Party line. Thus, it is this demand for total submission which is at once the Party's strength and principal weakness.

An Address By BENJAMIN MANDEL, *Research Director, U. S. Judiciary Sub-Committee on Internal Security*

I would like to have you join with me in a rather gruesome operation; namely, a lobotomy of the brain of communist, to find out what makes him tick.

At the outset let me point out, however, what the communist usually is not. He is not the ordinary type of low grade criminal, the common murderer or thief, although in effect he is far more dangerous to society. Note the example of Ethel and Julius Rosenberg whose devotion to the communist cause led them to transmit atomic secrets to the Soviet government. Strange to say, the communist may commit such a despicable crime inspired by humanitarian idealistic motives under the influence of a warped, ruthless and ungodly philosophy, a philosophy under which the end justifies any means.

The story is even told that an American communist was once asked what he would do if his city were destroyed by an attack of Soviet atomic bombs. Without winking an eyelash he replied: "I know I'll fry but I am sure I'll love it."

An understanding of the problem and proper dealing with the communist requires all the firmness of the efficient law enforcement officer, plus the patience, flexibility and understanding of the psychiatrist and the social worker. I say this because it is possible, under favorable circumstances and the use of correct methods, to convert a communist into a valuable and constructive member of the community. Whittaker Chambers, author of "The Witness" which I am sure you have all read, is a notable case in point.

Nor is the American communist necessarily moved to join the party as a result of actual poverty, a theory popular in certain ill-informed circles. Frederick Vanderbilt Field, a scion of the Vanderbilt family, was a columnist for the *Daily Worker*. Lement U. Harris, son of a wealthy Wall Street broker, is the party's agricultural expert. Huntington Hartford, heir of the A & P millions, was for a time a writer for the communist *New Masses*. Two of the wealthiest states in the union, New York and California, have been for years the leading states in terms of communist membership.

Cases have been known where youngsters of wealthy families have joined the communist movement because of a certain guilt complex, a feeling that they are enjoying ill-gotten riches which they have not rightfully earned or deserved. In retribution they feel called upon to ally themselves with those they consider the victims of sinful exploitation, namely, the workers. These individuals join the communist movement under the delusion that it is truly dedicated to the advancement of the interests of those who toil. They may even go to work in a factory, live the life of a worker, and dress in overalls. The fact of the matter is that American labor has overwhelmingly repudiated communism and the Soviet Union, which calls itself the Workers' Republic.

Sometimes a young man, devoid of any responsibility or discipline at home, will join the communist movement out of sheer boredom or a yearning to submit himself to some organization which demands discipline and obedience.

The communist you encounter may be an unsuccessful lawyer, writer, scientist or professional who convenienty attributes his own failure to the evils of the capitalist system under which he lives. He joins the communist movement to inflict a bitter revenge upon society. He hopes for vindication in the future under a communist regime. He receives recognition and responsibility from the Party. He detests everything connected with our way of life, our Government, our press, our churches, our schools and our institutions generally. On the other hand, he glorifies only one country, the Soviet Union, which he considers a model society for which he is ready to sacrifice everything.

Again the communist under investigation may be a young man who, because of unhappy home conditions or because he has arrived at the age of adolescence, decides to rebel against parental authority. He may be a college student away from home for the first time. He joins the Party with the feeling that he has become part of a great international movement bigger than his family. In many cases the youngster breaks with his family and voluntarily accepts the discipline of the party. He is trained by the party and given responsibility which feeds his ego. He feels superior to his family since he has found a philosophy and an organization that knows all the answers. As a case in point, some years ago the *New Masses* carried an article by the son of a conservative college professor. The article was entitled "My Father Is a Liar."

It is a recognized fact that a number of individuals join the Communist Party in response to certain neurotic needs. There are those who are poorly related to their surroundings, lonely individuals who feel rejected, who find a haven in the companionship provided by the Party and a source of moral support from its collective life and activity. The rebellious, antagonistic and hostile types find an outlet in a movement which is against our social order, a movement which is fundamentally destructive and violent. The Bohemian or gypsy-type who wants to be different welcomes a movement which is a challenge to all our established moral and social standards.

Contrary to its own professions and illusions held in certain liberal circles, the Communist Party is not primarily a party of workers. It consists in large measure of mission-minded intellecuals. The worker who joins may be moved by a number of special considerations. He may be a member of a communist-controlled union or fraternal organization in which Party membership may bring material benefit in terms of an official union post or an attractive industrial job. He may have been drawn into the Party during the depression considering the Party an instrument to fight unemployment. He may be foreign born or a Negro, resentful of certain treatment he considers discriminatory and laboring under the delusion that the Party is a vehicle to remedy this situation and advance the interests of that particular group. . . .

We have discussed why certain individuals join the Party. Now let us consider what happens to an individual after he joins. In effect he seals himself off hermetically in an ideological world utterly foreign and hostile to our own. It is as if he were living on another planet. The first stage of the process of divorcing himself from his former world is one of indoctrination in the principles of Marx, Lenin, Stalin and Khrushchev, in which process he is thoroughly brainwashed to the point where his framework of reference on all matters pertaining to his surroundings is turned inside out. This indoctrination gives him the sure answers to all questions. He becomes a mental robot trained not to think for himself but to give automatic responses to the slogans and directives handed down to him by the Party. He responds to his signals like the old firehorse or the trained football player.

The communist may raise a great fuss about the violation of civil liberties in the United States. But for some curious reason the party overnight reverses itself from support of the democracies to adherence to the Stalin-Hitler Pact, the communist libertarian utters not a word of protest but meekly submits to the reversal without even discussion or debate.

Our country becomes to his warped mind imperialist, war-mongering, Fascist, anti-labor and reactionary as compared with the Soviet Union which appears in roseate colors as peace-loving, democratic, anti-imperialistic, progressive, pro-labor and anti-Fascist. The employer and his subordinates are no longer creatures of flesh and blood, with human sympathies and understanding, but members of the hated capitalist class to be fought and ultimately destroyed. The press, says the indoctrinated communist, is prostituted by the ruling capitalist class and should not be believed. Religion, he holds, is the opium of the people used by the capitalist class to mislead and confuse the workers. The communist feels himself part of a heroic ultimately victorious army surrounded on all sides by enemies against whom he must be constantly vigilant and aggressive.

For his news and views, the communist relies primarily upon the communist press, the "Worker," the "People's World," "Masses and Mainstream" and "Political Affairs." His intimate associates are fellow communists. Outside associations are merely for purposes of exploration, propaganda, organization and recruiting. He divorces himself from all contacts which do not further his communist activity

When it suits the communist's purpose he will even join a church. Young communists have been known to join young people's church leagues in order to secure representation as bona fide church delegates at youth conferences. There are clergymen who are open or concealed members of the Communist Party. Party members actively penetrate American churches of national groups from behind the Iron Curtain where religion is state controlled and the church has become an arm of the communist government. Within various religious denominations, the Party supports its own religious fronts.

The Communist Party and its auxiliary organizations supply the comrades with a constant round of meetings, social activities, dances, camps, plays, lectures, concerts—all within the Party orbit. There is not an idle moment left during which he might do some thinking on his own or establish some outside contacts. The communist reads only books prescribed by the Party. . . .

The devout communist does not have close personal friends. His whole life is devoted to the Party in which relations are impersonal and strictly business. Besides the Party is so honey-combed with inner intrigue and surveillance that no Party member knows whom he can trust with his innermost thoughts and feelings.

Although he may be at heart a humane and kindly person, he is compelled by the logic of his communist doctrine to be utterly ruthless and inhuman when communist policy demands it. When, for example, millions of Russian peasants were being slaughtered during the campaign for collectivization, the communist blithely dismissed the issue with the remark, "You have to break the eggs to make an omelet."

Communist indoctrination brings with it a certain group conceit and pride. "We communists," they say, "are people of a special mold. We have the only true science of society. History is on our side."

A recruit may join the Party for some idealistic or doctrinal reason or because he has suffered from unemployment or because he was convinced of the Party's militancy in the trade union field, without appreciating that he is actually taking part in a Soviet-

inspired conspiracy against our Government. But as he becomes more and more deeply involved he cannot escape awareness of that fact Some glory in the excitement, in the atmosphere of conspiracy, the aliases, the secret groups of three or five, all of which are justified and glorified by communist teachings. Others, who may become alarmed, find themselves so deeply involved that they cannot break away.

How are we to know, then, that we have a communist in a given industrial plant, office or Government agency. Certainly he does not blazon forth his affiliations. He may even have no formal affiiliations of any kind for strategic reasons and be assigned to work undercover.

Let me add at this point that communist penetration in strategic industrial plants is not a matter of happenstance. Certain industries are carefully chosen by the Party for colonization purposes. The Party member, who may even be a college graduate, is sent by the Party after careful training to carry on communist activity in a given industry. I know of one case where a communist college graduate from New York conversant with a number of foreign languages, became a switchman on a southern railroad. Communist college boys have been active in the maritime industry, which is highly strategic from a communist viewpoint. I believe that the Party has allocated a number of its leading members in the aircraft industry of California at the present time. They have disappeared without a trace from their usual eastern haunts. This may sound fantastic to the average American who believes that all of us are free to choose our own way of life. But it is not fantastic to the communist who follows the rules laid down by the Party's authoritative "Manual on Organization" which declares:

> ***"A professional revolutionist is ready to go whenever and wherever the Party sends him. Today he may be working in a mine, organizing the Party, the trade unions, leading struggles; tomorrow, if the Party so decides, he may be in a steel mill; the day after tomorrow, he may be a leader and organizer of the unemployed . . . From these comrades the Party demands everything. They accept Party assignments—the matter of family associations and other personal problems are considered, but are not decisive. If the class struggle demands it, he will leave his family for months, even years . . . Our task is to make every Party member a professional revolutionist in this sense."***

How can we spot the communist who may be hiding in an important industrial plant or Government agency under a number of aliases with false references and credentials? In the first place, the communist, wherever he is, usually keeps contact with his lifeline, the weekly "Worker," which is his indispensable source of information and guidance. He may secure the paper by subscription, through a mail drop or through some Party intermediary. He may contact the Party, pay his dues and receive instructions through a specially assigned funcionary possessing a suitable cover. He may establish contact by traveling periodically but mysteriously to Party headquarters in a nearby large city or in New York. If he holds an office in a communist-controlled union, you can rest assured that he has the confidence of the Communist Party bosses.

The communist can be identified by his chip-on-the-shoulder attitude. He is always looking for grievances. If none exist, he will manufacture them. He never loses an opportunity to raise these issues in union and shop meetings. He is expert and tenacious in negotiations with the employers in order to win the confidence of his fellow employees. But he is not interested in adjustments and agreements. He is interested in keeping the plant in a constant turmoil. The issues of wages, hours and working conditions are merely incidental. Remember, he feels himself at all times a soldier on duty on the front lines of the class war.

In his shop and in his union the communist will raise from time to time issues which have little or no relation to wages, hours and working conditions, but which are being currently promoted by the communist press which, by the way, is "must" reading for a security officer. Among such issues are: cessation of atomic tests, civil rights in the South, defense of communist cases, recognition of communist China, peaceful co-existence with, and praise of, the Soviet Union. Occasionally he may distribute to his fellow shop members literature espousing these causes or leave such publications in locker or tool rooms.

The communist undercover agent may assume the guise of a disarming, back-slapping good mixer, a devout church member, an active trade unionist and a public-spirited citizen but beneath it all he instinctively inspires distrust.

If the plant manufactures some highly strategic product, the communist may reveal himself by his inquisitiveness into matters which are apparently not his business. Remember that a communist can make good use of even a seemingly nonsensitive position.

The individual under consideration may possess unexplained sources of funds which he uses for his various activities.

He may attempt to solicit a fellow shopmate for Communist Party membership or support of some communist front or campaign, or for a subscripion to a communist publication.

The personnel officer should by all means know the wife of a suspect. She may be the chief communist driving force in the family. She may be his source of contact with the Party. In fact, cases have been known where such aggressive Red Amazons have been assigned to marry strategically important Party members in order to hold such members to the Party line and accelerate their activities.

Of course, we should not overlook the possibility that the individual under investigation may have a criminal record in connection with communist activity, possibly under some other name and in some other locality.

We have also the possible case of the neurotic and maladjusted individual, who may have superior mechanical skill, but who, nevertheless, has become the tool of communist subversion.

If I were a security officer, I would watch with considerable interest all so-called forums and study groups operating in my local area. The study group has been one of the outstanding instruments of the party for attracting recruits. Agents involved in the Canadian spy ring were in many cases enlisted through study groups.

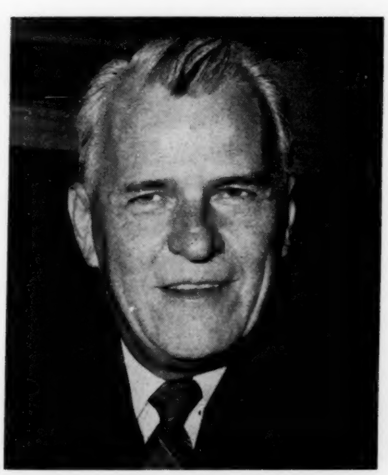
FIRST VICE PRESIDENT
JOHN L. BUCKLEY
VARIAN ASSOCIATES

SECOND VICE PRESIDENT
ERIC L. BARR, JR.
GENERAL DYNAMICS CORP.

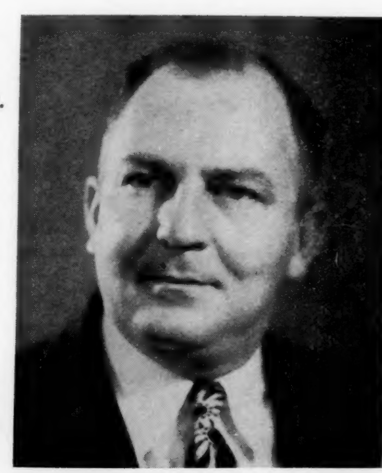
ASIS OFFICERS

1958 1959

PRESIDENT
RICHARD J. HEALY
RAMO-WOOLDRIDGE CORP.



SECRETARY
RICHARD E. SMITH
CHANCE VOUGHT AIRCRAFT, INC.



TREASURER
LAWRENE P. BUCHMAN
THE MARTIN CO.